MAGAZINE
NETWORK SET
السنة الأولى - شهر ايار/مايو الموافق لعام 2010
أول مجلة عربية تختص بأمور الشبكات تصدر من موقع WWW.NetworkSet.net

تعرف على تقنية Virtualization

- توفير المال والوقت والطاقة
- سهولة في التحكم والأعداد
- أمان وحماية عالي المستوى

نتائج الأستفتاء

ماهو أفضل منتدى عربي للشبكات ؟

- منتديات عرب هاردوير 87%
- منتديات برامج نت 3%
- منتدى بوابة العرب التعليمية 5%
- منتديات آخرى 5%

تقرير كامل عن محاكي الشبكات الأول + أسرار وحلول GNS3

تقرأون في هذا العدد

شاهدوا أيضا أقسام

2

networkset.net

أفتتاحية العدد

أطفال السكيورتي!

لا أعلم أن كانت هذه صدفة أم أن هذا الشيء هو واقعي ففي كل يوم أتجول فيه على المنتديات العربية أتفاجئ بأن الأغلبية تركض وراء دراسة كورسات السكيورتي والأمن مع أنه الطلب على هذا النوع من الوظائف ليس بالكبير في ساحتنا العربية وحتى عندما أحادث بعض الأشخاص عبر الماسنجر أجد نفس الشيء أريد أن أختص بمجال الأمن والسكيورتي و.....الهكر....ومن هنا بدأنا ومن هذه النقطة عدنا إلى النقطة الحقيقية وراء وجود الكثير من الأشخاص يهمهم دراسة هذا الكورس فكما هو معروف عند الأشخاص العاقلين أن 97% من العرب همهم الأول والآخر أن يكون هكر وقرصان زمانه وقد تستغرب آذا قلت لك أن هذه النسبة سوف تزيد لو في حال سألت أي شخص يدخل الأنترنت حول القرصنة وأمور الهكر فالكل سوف يرد عليك بأنه يعرف ويعلم الكثير حول هذه المواضيع وله الكثير من التجارب.

وفي أحد المرات وعلى أحد المنتديات المعروفة وجدت شخص يسأل سؤال حول مستقبله ويقول فيه أرغب في الدخول في مجال الأمن لاني أهوى هذا المجال وأحس نفسي بأني ناجح في هذا المجال ومشكلتي أني لا أعلم كيف أبدا فبماذا تنصحوني أن أبدا ؟وطبعا الشباب لم تقصر معه ومع طموحاته وقامت بوضع سلسلة كورسات قوية ومفيدة في هذا المجال وعندما عاد صاحبنا سأل سؤال في غاية الغباء وهو طيب أذا أنا درسة أول ثلاث كورسات هل أستطيع أن أكون هكر قوي؟؟؟ أو تجد أحدهم يطلب منك كورسات السكيورتي التى تفيد في تعلم القرصنة بشكل مباشر

نعم أخي هذه أحد الأمثلة وهناك منها الكثير وبرائي أن أتجاه الأشخاص نحو السكيورتي والأمن يتجلى في عدة أسباب منها

أ-تعلم القرصنة من أجل التباهي والتفاخر بقوته وبذكائه أمام الناس أو من أجل تحرير فلسطين وتدمير أمريكا من خلال أغلاق بعض المواقع وطبعا لن ينسى أن يضع أسمه المرمز مثل هذا الأسم الذي صادفته في أحد المرات|-|$@|><| ومعناها الحرفي كلاش!!!

ب-التأثر بأفلام هوليوود مثل أفلام القرصنة والسرقات وعملية أختراق البنوك ومحاولة تقليد هذه الخرافات !

ج-وهو الشخص الطبيعي الذي تعلم الأساسات وتعلم البرمجة والشبكات بالأضافة إلى التعامل مع الأنظمة الحرة مثل لينوكس وعائلته المحترمة وآخيرا أنصح جميع الأشخاص الذين يفكرون في هذا المجال أن ينظروا إلى هذه الشهادة من مفهوم أكبر وأن يبدأوا بتطوير أنفسهم من خلال تعلم الأساسيات المطلوبة لهذا المجال وأن يبتعدوا عن فكرة القرصنة والتخريب وأتخذ هذا المقولة الأنكليزية كشعار لك Hack to learn not learn to hack

ويبقى السؤال موجود في زهني هل هي مصادفة أم هو واقع نعيش فيه؟؟؟

ودمتم بود

المحررون الدائمون

- الدكتور محمد التميمي
Yarra_link@yahoo.com
- المهندس أيمن النعيمي
admin@networkset.net
- المهندس أحمد الشحات
warior10@hotmail.com
- المهندس عادل الحميدي
adel_husni2000@hotmail.com
-
-

المحررون الضيوف

- المهندس عثمان أسماعيل
othman_ucmael@yahoo.com
-
-
-
-
-
-

موقع المجلة
www.networkset.net
بريد المجلة
magazine@networkset.net
بريدي الخاص
admin@networkset.net

محتويات أيار 2110

حصاد الشبكة العنكبوتيه لعام 2009

بقلم محمد التميمي

رغم الكم الهائل من التغيرات والتطورات التي تحدث في عالم الإنترنت فان الجانب الإحصائي لهذه التغيرات تكاد تكون منعدمة ولهذا قامت شركة بينجدوم بنشر مقالة عرضت فيها إحصائيات شبكة الإنترنت في عام 2009. مستعينة بمجموعة متنوعة وواسعة من المصادر من مختلف أنحاء الشبكة علاوة على إضافة المزيد من المعلومات التي رصدتها الشركة بنفسها. كم من المواقع الإلكترونية تم إضافتها على شبكة الإنترنت؟ كم بريداً إلكترونياً تم إرساله؟ كم بلغ عدد مستخدمي الإنترنت فى 2009؟ هذا الموضوع سوف يجيب على جميع هذه الأسئلة وغيرها من الاسئلة الكثيرة ذات العلاقة.

- 234مليون موقع 126مليون مدونة...
- 1.73 مليار عدد مستخدميها عالميا
- 90تريليون رسالة إلكترونية...
- 4مليار صورة... ومليار مقطع فيديو يومي.

البريد الالكتروني

- عدد رسائل البريد الإلكتروني المرسلة على شبكة الإنترنت في عام 2009 بلغ 90تريليون رسالة.
- متوسط عدد رسائل البريد الإلكتروني المرسلة يوميا 274مليار.
- عدد مستخدمي البريد الإلكتروني في جميع أنحاء العالم 1.4مليار.
- عدد مستخدمي البريد الإلكتروني الجدد منذ العام قبل الماضي 100مليون.
- 81٪ نسبة رسائل البريد الإلكتروني "المزعجة" من إجمالي عدد رسائل البريد الإلكتروني المرسلة في عام 2009.
- 24٪ نسبة الزيادة في عدد الرسائل المزعجة مقارنة بالعام السابق.
- عدد الرسائل المزعجة "غير المرغوب فيها" المرسلة يوميا 200مليار على افتراض ان 81٪ من الرسائل الإلكترونية المرسلة كانت مزعجة.

المواقع الإلكترونية

- 234مليون عدد المواقع على شبكة الإنترنت حتى ديسمبر 2009
- 47مليوناً عدد المواقع الإلكترونية التي تم إنشاؤها في عام 2009

خوادم الويب

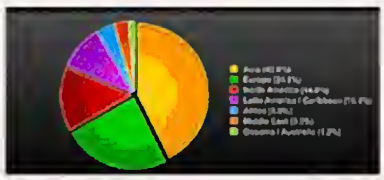
- 13.9٪ نسبة الزيادة في الخوادم التي تستخدم الاباتشى Apache في عام 2009
- 22.1٪ نسبة الزيادة في خوادم الإنترنت التي تستخدم IIS.
- 35.0٪ نسبة الزيادة في خوادم الإنترنت التي تستخدم جوجل GFE.
- 384.4٪ نسبة الزيادة في الخوادم التي تستخدم Nginx.
- 72.4٪ نسبة الزيادة في الخوادم التي تستخدم Lighttpd.

أسماء النطاقات

- وصل عدد النطاقات التي تستخدمCOM 81.8مليون نطاق مع نهاية 2009
- عدد النطاقات التى تستخدمNET 12.3مليون
- عدد النطاقات التي تستخدمORG 7.8مليون
- عدد نطاقات البلدان مثل CN, UK, DE ect. بلغ 76.3مليون
- 8% نسبة الزيادة في أسماء النطاقات مقارنة بالعام السابق

مستخدمو الإنترنت

- 1.73مليار عدد مستخدمي الإنترنت حول العالم حتى سبتمبر 2009
- 738.257.230عدد مستخدمي الإنترنت في آسيا
- 418.029.796عدد مستخدمي الإنترنت في أوروبا
- 252.908.000عدد مستخدمي الإنترنت في أمريكا الشمالية
- 179.031.479 عدد مستخدمي الإنترنت في أمريكا اللاتينية ومنطقة البحر الكاريبي
- 67.371.700عدد مستخدمي الإنترنت في أفريقيا
- 57.425.046عدد مستخدمي الإنترنت في الشرق الأوسط
- 20.970.490عدد مستخدمي الإنترنت في أوقيانوسيا/ أستراليا
- 18٪ نسبة الزيادة في عدد مستخدمي الإنترنت مقارنة بالسنة الماضية



الشبكات الاجتماعية

- بلغ عدد المدونات على شبكة الإنترنت 126مليون مدونة
- 27.3مليون تدوينة قصيرة تضاف يومياً إلى "تويتر" حتى نوفمبر 2009
- 57 % من مستخدمي تويتر هم من سكان الولايات المتحدة الأمريكية
- 350مليون عدد مستخدمي فيس بوك
- 50%من مستخدمي فيس بوك يقومون بالاطلاع على ملفاتهم بشكل يومي
- 500.00عدد التطبيقات الفاعلة فى فيس بوك

الصور

- عدد الصور التي تم حفظها في فليكر 4مليار صورة أكتوبر 2009
- عدد الصور التى يتم تحميلها شهرياً على فيس بوك 2.5مليار أي 30مليار صورة يتم حفظها سنويا على فيس بوك

الفيديو

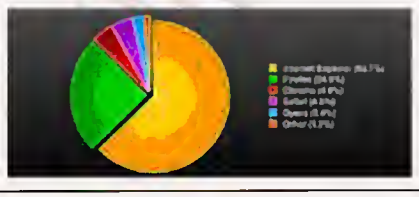
- عدد مقاطع الفيديو التي تتم مشاهدتها يومياً في يوتيوب حول العالم (مليار مقطع)
- عدد مقاطع الفيديو التي تتم مشاهدتها شهرياً في يوتوب في الولايات المتحدة الأمريكية (12.2مليار) مقطع (نوفمبر 2009)
- عدد مقاطع الفيديو التي تتم مشاهدتها شهرياً في "هولو" في الولايات المتحدة الأمريكية (924مليار) مقطع (نوفمبر 2009)
- 182متوسط عدد مقاطع الفيديو التي يشاهدها مستخدم الإنترنت الواحد فى أمريكا

البرمجيات الخبيثة

- 148.000جهاز كمبيوتر يصاب يوميا بمواد خبيثة
- 2.6مليون مادة خبيثة تهدد الأجهزة في بداية 2009(فيروسات وديدان)
- 921.143عدد توقيعات الشفرات الخبيثة التي أضافتها سيمانتيك Symantic

متصفحات الإنترنت

- 7.26٪ لمتصفح انترنت اكسبلورر
- 6.42٪ لمتصفح فايرفوكس
- 6.40٪ لمتصفح قوقل كروم
- 5.40٪ لمتصفح سفاري
- 4.20٪ لمتصفح أوبرا
- 2.10٪ لمتصفحات أخرى



تقرير كامل حول محاكي الشبكات الأول

بقلم أيمن النعيمي

يعد برنامج الـGNS3 هو البرنامج الأول في عالم المحاكيات نظرا للتسهيلات الكبيرة التى قدمها لكل دارسي الشبكات في العالم من خلال توفير منصة قوية لمحاكات أجهزة سيسكو سابقا وأجهزة جونيبر لاحقا التى تم أضافتها إلى الأصدار الأخير منها .

ونظرا لأهمية هذا البرنامج سوف أحاول في هذا الموضوع أن القي الضوء على كيفية تنصيب وتشغيل البرنامج بالأضافة إلى ذكر أكثر المشاكل شيوعا في هذا البرنامج كما سوف يكون هناك بعض الأضافات والأسرار الخاصة فيه والتى تساعد في زيادة كفاءة وعمل البرنامج .

الـ GNS3 ببساطة هو ليس برنامج محاكي للشبكات كما يظن الأغلبيةلانه فقط عبارة عن واجهة رسومية لمحاكي الشبكات الـ Dynamipsوهو برنامج مفتوح المصدر يعمل على جميع أنواع الأنظمة من بينها ويندوز ولينوكس وماكنتوش ولكي يعمل يحتاج الى 3أشياء مهمة

أولا يحتاج طبعا الى الـ Dynamips والذي يعد بدوره قلب النظام الذي سوف يقوم بمحاكاة أنظمة سيسكو من خلال محاكاة الـ IOS

ثانيا يحتاج الى الـ Dynagen وهو صلة الوصل بين قلب النظام Dynamips والمستخدم وتتم عبر نقله الأوامر الكتابية من وإلى

ثالثا يحتاج الى برنامج WinPcap وهو برنامج يقوم بالتقاط ونقل الـ Packet في الشبكة عبر مجموعة من البروتوكولات

رابعا غير مهم لكن أذا في حال أردت أن تقوم بعمل محاكي للجدران النارية الخاصة بسيسكو أو جونيبر فأنت تحتاج الى برنامج Qume

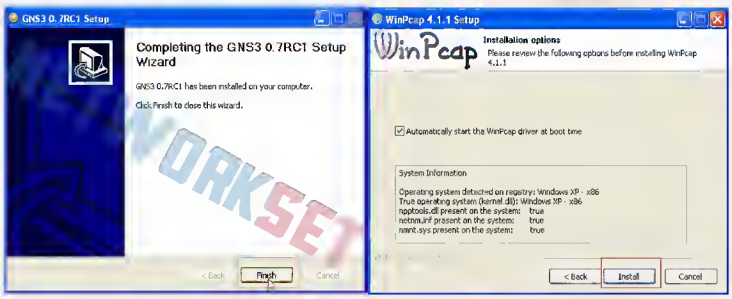
طريقة التنصيب (لويندوز فقط)

نقوم أولا بتحميل آخر نسخة من البرنامج ولا نحتاج إلى أي شيء آخر لان مع البرنامج يأتي الداينامبيس والدايبجين كما سوف نرى في الشرح

وللتحميل سوف نتوجه الى رابط الموقع

http://www.gns3.net/download

ونختار آخر إصدار ونقوم بتحميله ونبدا التنصيب بأول الخطوات

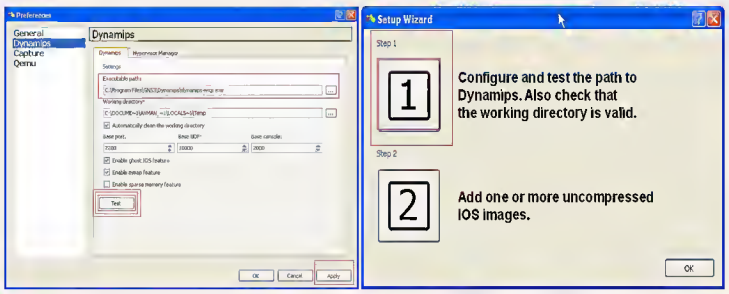


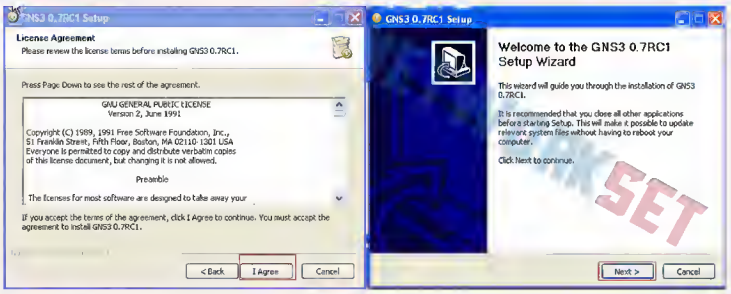
بعد أن أنتهينا من التنصيب يلزمنا نسخ IOS لكي نضيفه للبرنامج وهي موجودة في كل مكان على الانترنت والشرح سوف يكون عن نسخة 3640

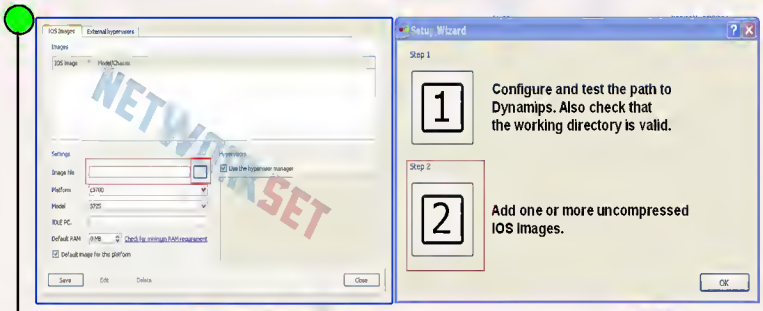
بعد تحميل النسخة من الانترنت نقوم بتشغيل البرنامج لأول مرة لنجد Wizardيطلب منا تنفيذ شيئان مهمان لضمان تشغيل البرنامج بشغل جيد

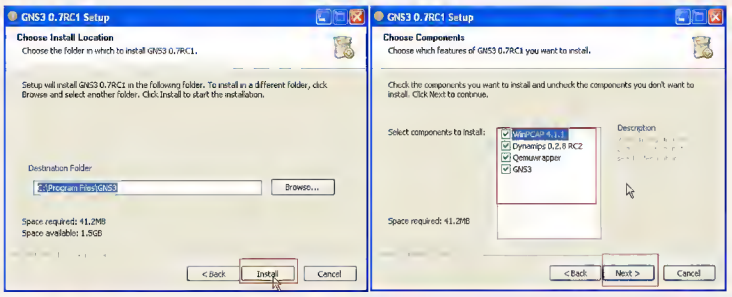
الأول هو التأكد من أن الداينامبيس منصب على الجهاز ويعمل مع الـ GNS3

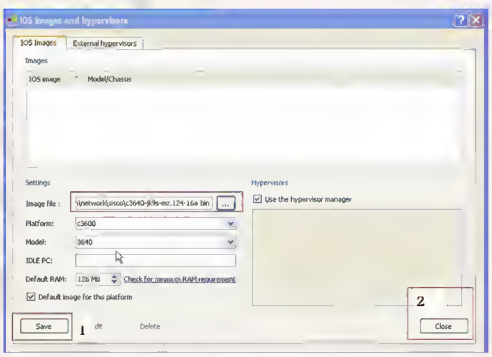
الثاني هو إضافة نسخة سيسكو IOS للبرنامج ولكي نقوم بتنفيذها نقوم بالتالي:

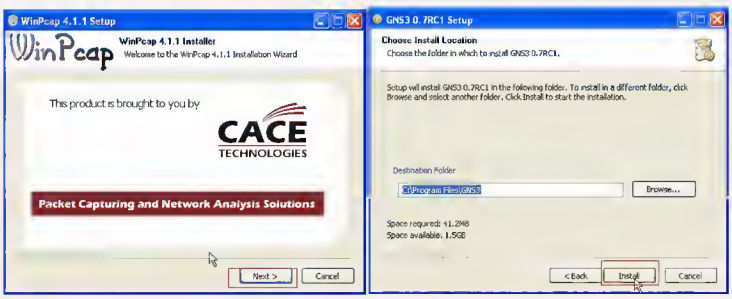












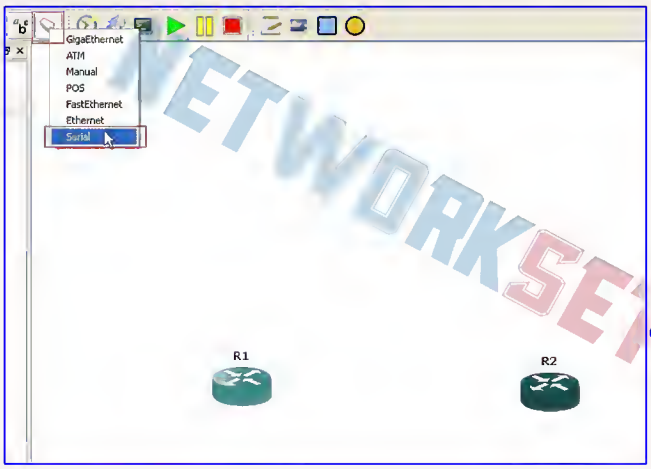
بعد أن أنتهينا من أعداد البرنامج لنتعرف على الـ ToolBar الخاص بالبرنامج

بعد ان تعرفنا على التوول بار لنبدأ الشغل العملي من خلال قيامنا بتطبيق محاكاة لروترين سوف نقوم أولا بسحب روتر 3600- من القائمة اليسرى الى وسط البرنامج

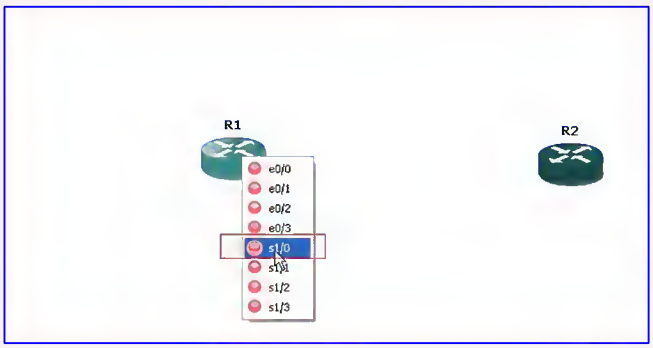
وبعدها نضغط بالزر اليمين على الروتر ونختار configure لنقوم بأعداد الـ SLOTS والتى نقوم فيها بأختيار عدد ونوع البورتات التى أريد أن استخدمها في الروتر ويمكننا أيضا تحدد كمية الرام وحجم الهارد دسك أو الفلاش الخاص بالروتر

NM-1FE لأضافة بورت واحد من نوع فاست ايثرنت
NM-1E لأضافة بورت واحد من نوع ايثرنت
NM-4E لأضافة أربع بورتات من نوع ايثرنت
NM-16ESW نقوم بأختيار هذا الـ Slot في حال أردنا أن نقوم بعمل محاكاة لسويتش لان الـ Dynamips غير مجهز لعمل محاكاة للسويتش
NM-4T لأضافة أربع بورتات من نوع سيريال

وبعد أن ننتهي من تحديد الـ slots نقوم بتكرار العملية مع روتر آخر وننتقل مباشرة إلى طريقة الوصل بين الروترين وللقيام بذلك يتوجب علينا أن نعرف أن أختيار كل التوصيل يعتمد على نوع الـ Slot الذي قمنا بأختياره وهي موضحة بالصورة

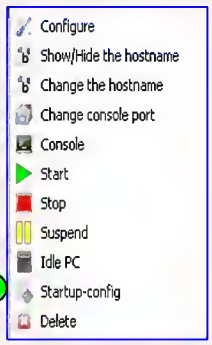


بعد تحديد الكبل نضغط على الروتر الأول ونختار رقم البورت

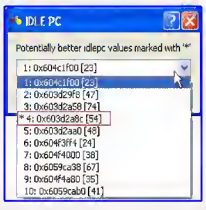


ونقوم بتوصيله مع الروتر الثاني بنفس الطريقة ولم يبقى علينا إلا أن نضغط على زر البدأ Start من التوول بار ليبدأ البرنامج عمله ويقوم بتشغيل عملية المحاكاة لكلا الروترين والتى لاتحتاج منك إلا الضغط على زر Console لكي تصل إلى موجه الأوامر الخاص بكل روتر.

أما بخصوص الخيارات الموجودة على كل روتر والتى نستطيع أن نراها من خلال الضغط بالزر اليمين على الروتر فهي كالآتي :



Configure لأعداد الروتر وقد تم التطرق لها من قبل
Show/hide لأخفاء وأظهار اسم الروتر من على التبلوجي
Change the hostname لتغيير اسم الروتر
Change console port لتغيير رقم الكونسول بورت
Console للأتصال مع الروتر بواسطة الكونسول
Start لبدأ تشغيل الروتر
Stop لأطفاء الروتر
Pause توقيف مؤقت



Idle PC وهي من أهم الأشياء وفائدتها تحديد قيمة معينه من المعالج تساعد في تخفيف الضغط عليه ويتم تحديده بان نقوم أولا بتشغيل الروتر وبعدها نضغط Idle PC ونتنظر قليلا لنرى عدة أرقام ونختار القيمة التى بجانبها علامة النجمة وكما هو موضح بالصورة

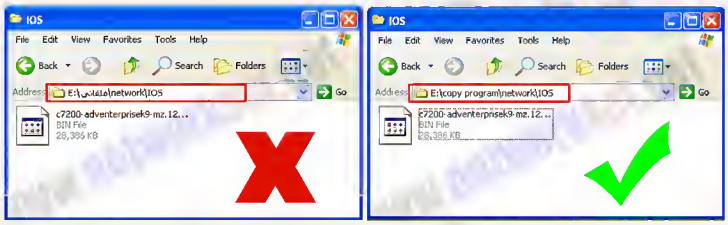
Startup-config لأختيار اسم معين لملف الأعدادات
Delete لحذف الروتر بشكل كامل

مشاكل وحلول وأسرار في برنامج الـ GNS3

سؤال: تواجهني هذه المشكلة عند تشغيل الروتر ؟

error 209 unable to start vm instance Ro

جواب: هذه المشكلة تحدث عادة عندما تقوم بإضافة ملفات IOS موجودة في مجلدات مكتوبة باللغة العربية أو لغة آخرى عدا الانكليزية ولايقتصر الموضوع على المجلد الموجود فيه النسخة بل يشمل كل الملفات التى تدخل في مسار النسخة وهذه بعض الأمثلة للتوضيح.



سؤال: قمت بإختيار قيمة الـ Idle PC لكن المعالج مازال يعمل بنسبة عالية ؟

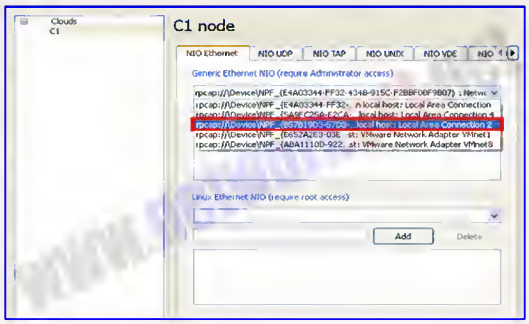
جواب: تحدث هذه المشكلة أحيانا من خلال البرنامج نفسه ويعود هذا الى خطأ في أستخراج القيمة المناسبة لذلك قم بالمحاولة أكثر من مرة حتى تجد المعالج قد بدا يعمل بشكل طبيعي ولاتنسى أن تختار القيمة التى بجانبها علامة نجمة.

سؤال: لماذا يأخذ الروتر وقتا طويلا حتى يعمل وكيف أستطيع إنقاص هذه المدة ؟

جواب: يأخذ الروتر وقتا طويلا بسبب قيامه بفك ضغط برنامج التشغيل IOS على الذاكرة ولكي نقوم بتشغيل الروتر في سرعة أكبر نقوم بفك ضغط نظام التشغيل على الهارد وبعدها نقوم بإضافته مرة ثانية على البرنامج وطريقة فك الضغط تتم كالتالي أضغط بالزر اليمين على ملف الـ IOS واختر فتح بواسطة أو Open with وقم بإختيار برنامج الوينزار وبعدها قم بإختيار فك ضغط الملف هنا وآخيرا قم بإضافة النسخة الجديدة إلى البرنامج مرة آخرى.

سؤال: كيف أقوم بربط البرنامج مع جهاز كمبيوتر آخر لتخفيف الحمل على الجهاز ؟

جواب: للقيام بهذا الموضوع قم بإضافة غيمة إلى الـ Topology وبعدها بالزر اليمين أختار أعدادات وقم بإختيار كرت الشبكة الموصول مع الجهاز الآخر كما هو موضح بالصورة وبعدها أضغط على كلمة ADD



سؤال: كيف أقوم بربط البرنامج مع برنامج الفي أم وير ؟

جواب: أول شيء يجب عمله هو أضافة لووب باك انترفيس على جهاز الكمبيوتر وبعدها نقوم بإضافة غيمة كما في السؤال السابق ونربطها مع اللوب باك انترفيس وبعدها نتوجه إلى برنامج الفي أم وير وندخل إلى Edit Virtual Network Editor ومن خيار Bridged to نقوم بإختيار اللوب باك انترفيس وآخر شيء نقوم بإعطاء أجهزة الكمبيوتر والانترفيس ايبيات تنتمي جميعها لشبكة واحد.

سؤال: لماذا لايحفظ البرنامج الأعدادات التى قمت بعملها على الروتر ؟

جواب: لكي يقوم البرنامج بحفظ الأعددات يجب عليك أولا وقبل تشغيل الروترات أن تتوجه إلى File New Project وقم بإختيار المكان التى سوف يقوم البرنامج بحفظ أعدادات الروتر وبعدها قم بوضع اشارة عند كل خيار موجود في نفس النافذة وهي خياران الأول Save NVRam والثاني Router Export

سؤال: كيف أقوم بربط برنامج الـ GNS3 مع برنامج SecuerCRT ؟

بعد تنصيب كل من برنامج الـ GNS3 و SecuerCRT على الكمبيوتر نقوم أولا بإنشاء ملف تكست جديد ونضع بداخله هذا الكود

```
#$Language=V"BScript   "
#$Interface="1.0"
Sub main
crt.window.caption=crt.arguments(0)
End Sub
```

بعد نسخ الكود داخل الملف نقوم بحفظه بإسم securecrt.vbs ونضع السكربت داخل مجلد الـ GNS3 والموجود على الامتداد التالي

C:\Program Files\GNS3

وأحب أن أونوه أن مكان الحفظ هام حتى يعمل السكربت بشكل جيد وبعدها نقوم بتشغيل برنامج الـ GNS3 ونضغط على Edit وبعدها نختار Preference وفي خانة الـ Terminal command قم بوضع هذا الكود

```
start  C:\progra~1\vandyk~1\SecureCRT\SecureCRT.EXE /script C:\progra~1\gns3\securecrt.vbs /arg %d /T /telnet %h %p
```

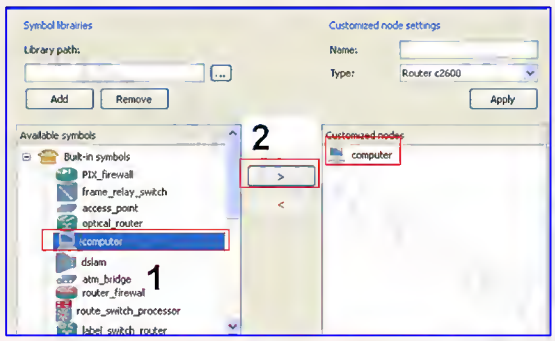
ملاحظة آخيرة لكي يعمل السكربت يجب مراعة مكان وجود برنامج الـ SecurCRT وهو على الامتداد التالي

C:\Program Files\VanDyke Software\SecureCRT

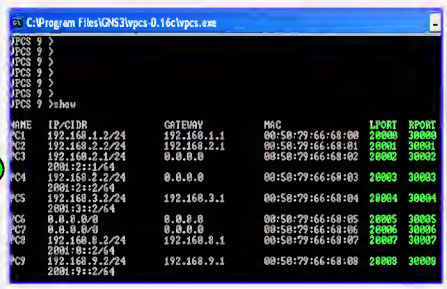
سؤال: كيف أقوم بربط البرنامج مع برنامج الـ VPCS ؟

جواب: قبل أن أعرض الطريقة سوف أشرح بشكل سريع ما هو برنامج الـ VPCS ؟ الـVPCS أحد البرامج المفتوحة المصدر التى تهدف إلى عمل محاكاة بسيطة جدا لنظام التشغيل من خلال دعم بروتوكول الـ Ping والـ Trace route وهي الأدوات الوحيدة تقريبا التى نحتاجها في اللابات التطبيقية بالاضافة إلى أنه يدعم الـ IPv4 و IPv6 كما أنه مزود بي DHCP client لتزويده بالأيبي بشكل أوتماتيكي ويستطيع أن يوفر لك 9أجهزة وهمية وهو يعد من أصغر أنظمة التشغيل البسيطة وحجمه 2ميغا فقط.

بعد تحميل البرنامج وفك الضغط عنه نقوم أولا بتشغيل السيرفر الخاص بالبرنامج وهو VPCS.exe وبعدها نقوم بتشغيل برنامج الـ GNS3 وهي ملاحظة هامة تشغيل السيرفر قبل برنامج الـ GNS3 وبعدها نتوجه مباشرة إلى Edit->Symbol Manager ونبحث في القائمة اليسرى عن صورة لجهاز كمبيوتر ونقوم بإضافتها إلى القائمة اليمنى كما هو موضح بالصورة

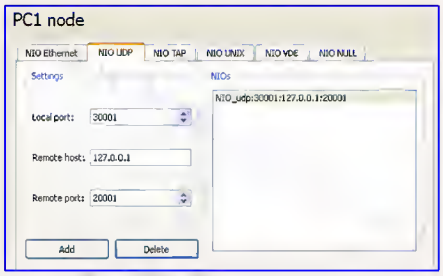


وبعدها نقوم بإختيار Cloud من خيارات الـ Type المتاحة ونضغط على زر Apply ونختمه بالضغط على ok



بعدها نتوجه إلى برنامج الـ VPCS ونقوم بكتابة الأمر showلتظهر لنا هذه النتائج والتى يهمنا منها آخر أثنان وهما Lportو Rport نقوم بحفظ أحدهم وليكن 30001 20001وتتوجه بعدها للمرة الأخيرة إلى برنامج الـ GNS3

أقوم أولا بإضافة روتر وجهاز كمبيوتر وبعدها أضغط بالزر اليمين على جهاز الكمبيوتر وأختار أعدادات وأتوجه إلى التبويب الثاني وأقوم بكتابة الأرقام السابقة بالاضافة إلى 127.0.0.1 في الصندوق الثاني.



وأرجو منكم أن تلاحظو معي أن في خيار LocalPort قمت بكتابة رقم Rport الموجود في البرنامج وفي خانة الـ RemotePort قمت بكتابة رقم Lport وإذا قمت بعكس الأرقام لن ينجح الاتصال

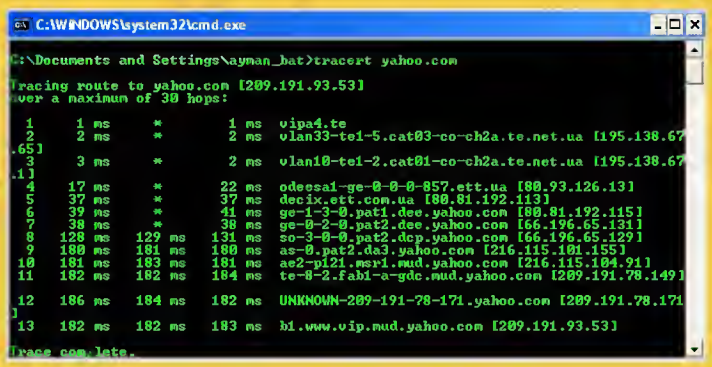
وبعدها نضغط على زر ADD وبعدها OK ونقوم بالتوصيل بين جهاز الكمبيوتر والروتر من خلال كبلFastEthernet ونقوم بتشغيل الروتر ونعطي المخرج الموصول مع جهاز الكمبيوتر أيبي وليكن 192.168.2.1/24وتتوجه مرة ثالثة إلى برنامج الـVPCS وتكتب في موجه الأوامر الرقم 2وهو يعني النظام التشغيل الثاني ونعطيه ايبي وماسك وغيت واي من خلال الأمر التالي ip 192.168.2.2 192.168.2.1 24وبهذا نكون قد أنتهينا

كيف تتم عملية التتبع في الشبكة

بقلم أيمن النعيمي

إستكمالا للسلسلة التى بدأت فيها بشرح الامر Ping وكيفية عمله سوف أستكمل معكم مع أمر آخر لا يعد أقل أهمية من الاول وهو الـ Trace route وأهميته تكمن في تحديد مكان المشكلة التى تمنعنا من الوصول الى الهدف وذلك بعرض المسار التى يسير فيها الباكيت للوصول الى الهدف وتحديد في اي النقط تقع المشكلة كما سوف نرى في المثال القادم وقبل ان أدخل في الموضوع أحب ان أقول ان هذا الأداة موجودة في كل انظمة التشغيل ففي ويندوز الامر سوف يكون tracert وفي لينوكس هو traceroute وفي أجهزة سيسكو هو ايضا traceroute

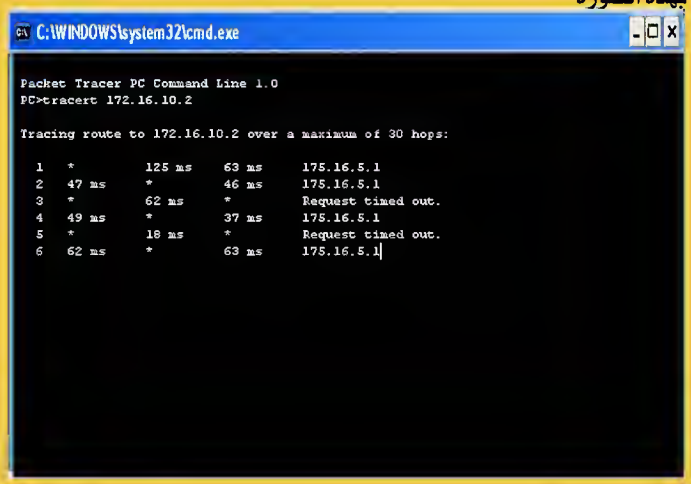
لنتعرف أولا على الامر على ويندوز ونرى كيف ستكون النتائج



وكما ترون قمت أولا بكتابة الامر وبعدها كتبت اسم الموقع hostname أو الايبي X.X.X.X المراد عمل التتبع عليه

اذا كيف تعمل هذه الاداة

تعتمد هذه الاداة كسابقتها الـ Ping على البروتوكول ICMP ومبدأ عملها يكمن في إرسال Echo Packet إلى الهدف لكن هذه المرة سوف يرسل الطلب ضمن شرط وهو ان TTL يساوي واحد لكي يضمن ان يرد عليه أول Hop في عملية التتبع وعندما يتم الاستلام تقوم بارسال طلب آخر لكن هذه المرة الـ TTL تساوي اثنان وبعدها 3 وهكذا الى ان يتم التتبع الى الهدف المطلوب طيب ماذا سيحدث لو كان هناك خلل في المسار وكانت النتائج كما هو موضح بهذه الصورة



لاحظ معي عند الرقم 3 ★ ★ معنى هذه النجوم ان الـ Next Hop الثالث في المسار لايقوم بالرد على الطلب القادم من الـ ICMP والاسباب كثيرة ولكن سوف أذكر أهمها :

وهو ان يكون هذا الروتر يحوي فايروول او اكسس ليست تمنع مرور هذه الانواع من الباكيت أي أنها تمنع الـ ICMP او هناك مشكلة في الروتر نفسه والاجابة من الروتر سوف تكون Echo بداخله الـ Type=11 والـ Code=0 وبناء على بعض الأقتراحات التى وصلتني بخصوص أن الجدول لم يكن واضحا في العدد السابق سوف أعيد نشره بشكل أكبر وأفضل

ICMP Message Types		
Type	Code	Description
0	0	Echo reply (تستخدم للرد على الطلب)
3	0	Destination network unreachable
	1	Destination host unreachable
	2	Destination protocol unreachable
	3	Destination port unreachable
	4	Fragmentation required, and DF flag set
	5	Source route failed
	6	Destination network unknown
	7	Source host isolated
	8-13	موجودة لكن غير مهمة جدا
4	0	Source quench
5	0	Redirect Datagram for the Network
	1	Redirect Datagram for the TOS & network
	2	Redirect Datagram for the TOS & network
	3	Redirect Datagram for the TOS & host
6	0	Alternate Host Address
8	0	Echo request (تستخدم الطلب)
9	0	Router Advertisement
10	0	Router discovery/selection/solicitation
11	0	TTL expired in transit
	1	Fragment reassembly time exceeded
12	0	Pointer indicates the error
	1	Fragment reassembly time exceeded
	2	Bad length
13	0	Timestamp
14	0	Timestamp reply
15	0	Information Request
16	0	Information Reply
17	0	Address Mask Request
18	0	Address Mask Reply

Character	Description
nn msec	For each node, the round-trip time in milliseconds for the specified number of probes
*	The probe timed out
A	Administratively prohibited (example, access-list)
Q	Source quench (destination too busy)
I	User interrupted test
U	Port unreachable
H	Host unreachable
N	Network unreachable
T	Protocol Unreachable
P	Timeout
?	Unknown packet type

وفي الجدول الثاني سوف نجد تفسير لبعض الرموز التى ممكن ان تصادفنا اثناء عمل التتبع.

وقبل أن أنهي الموضوع أحب أن أقول ان جميع الارقام لموجود بجانبها ms في النتائج تدل على الفترة الزمنية لذهاب ورجوع الطلب يعني لو نظرنا الى الصورة الثانية عند الرقم 2 سوف نجد ان الطلب وصل في 74 مللي سكوند بينما فترة الرجوع استغرقت 64 مللي سكوند

من أين أبدأ وكيف أبدأ في الشبكات ؟؟؟ سؤال لطالما حيرني !!!

بقلم: عادل الحميدي

سؤال لطالما تكرر في الكورسات والمنتديات من الأفاضل الأعضاء وخصوصا الشباب ، أو ممن قرأ في المجال أو سمع عنه وأعجبه ، أو أراد أن يطور من نفسه للحصول على وظيفة أفضل وخصوصاً في مجال الـ IT تكنولوجيا المعلومات ، والذي أُشتهر عنه أنه أعلى المجالات رواتب وأقلها في ساعات العمل فزاد الإقبال عليه .

وهو في الحقيقة سؤال محير فعلاً ، فكلنا في البداية مر به هذا السؤال وتلك الحيرة ، ففي بداية الطريق يكون الشخص متخوف وتائه وحيران لما يسمع من كلام كثير وبعض هذا الكلام يناقض بعضه بعضا ، وهو لا يدري أين الصواب ؟ ولا أين الإتجاه الصحيح ؟

بل هناك من يزيده هذا الكلام الكثير حيرة على حيرته وخوف على خوفه ، حتى إن بعضهم يحكي لي أنه جلس ثلاث سنوات محتار لا يعرف كيف يبدأ ؟ بل وبعضهم قرر أن هذا المجال محال وهرب بجلده كما يقولون ...

من أين يبدأ وكيف يبدأ ؟ وما هو المفيد حسب الموقع الجغرافي) بلد الإقامة أقصد لأن كل بلد لها ظروفها الخاصة (؟

قد يقول البعض لعل هذا المقال سيزيدني حيرة فوق حيرتي سأغلقه ×××

أنصحك لا تفعل إستمر معي للنهاية وسترى النور بعينيك ، فوالله الذي لا إله غيره ما كتبت هذا الكلام إلا بعد عناء طويل أخذ من عمري سنين بل أستطيع أن أقول أني رويت بداية هذا الطريق بدمي ، فبدل أن تضيع مثل هذه السنين وهي غالية إسمع مني لدقائق لعلك تستفيد ...

إتفقنا إذن لنبدأ ...

أسئلة كثيرة تدور في خلد المبتدئين ولا يعرفوا لها إجابة وأحببت أن أنزع فتيل هذه الحيرة حتى أفجر تلك الطاقات المكبوتة عند شباب المسلمين حتى يشعلوا نهضة هذه الأمة من جديد .

ولا أعرف إن كان أحد الأفاضل قد سبقني وأدلى بدلوه في مثل هذا الموضوع أم لا ؟؟؟ ولعلي أستفيد ، لكن هو جهد المقل فما كان فيه من خطأ فمن نفسي ومن الشيطان ، والله ورسوله منه براء ، وما كان فيه من توفيق فمن الله وحده لا شريك له .

كما أن هذا يعبر فقط عن وجهة نظر خاصة وشخصية تكونت لدي من خلال سنين الخبرة قد يوافقني فيها البعض وقد يختلف معي فيها آخرين ، والخلاف لا يفسد للود قضية .

وحتى وإن كان أحد أجاب قبلي على مثل هذه التساؤلات لكن ما رأيت أحداً أفرد لها موضوعاً مستقلاً بل سلسلة من المقالات ، فأردت أن أجعلها سلسلة مستقلة من المقالات تحت نفس هذا العنوان بحيث يحيل إليه الإخوة الأفاضل أي أحد من الشباب الجدد والذين يسألون مثل هذه التساؤلات ؟؟؟

وأرجو من الله العون والتوفيق ، اللهم مدني بمدد من عندك

أعرف أني أطلت عليكم في مقدمتي لكن كما يقولون " اللي أوله شرط آخره نور " ، ولنبدأ

خلك طموح

وأقول بعد باسم الله فكل عمل لا يبدأ فيه باسم الله فهو منزوع البركة ، يلا نخطط لمستقبل باهر ...

دعنا نتفق منذ البداية على أننا نريد البداية الصحيحة والتي يتم فيها التأسيس المتين لمستواك العلمي والعملي ثم نتدرج حتى نصل إلى مستوى الاحتراف ثم الخبير ، ولا نريد الاستعجال فما بني على باطل فهو باطل ، وليس معنى هذا أننا سننهي عمرك كله ولن تستفيد لا وألف لا ، بل سأضع أنا وأنت خطة زمنية محددة بوقت ننهي خلالها كل ما نريد وهذا شيء مهم جداً جداً وبعد هذه الفترة نكون وصلنا لمستوى الخبراء وحتى تكون مميزاً بصدق ، ومن سمات هذه الخطة الزمنية أن تقف بعدها مع نفسك وتحاسبها تكافئها إن أنجزت وأحسنت وتعاقبها إن أساءت ، وتقيم تلك المرحلة تتعلم من أخطاءك وتستفيد خبرة والله المستعان ...

دعنا نقول من الآن وإن كان هذا سابق لأوانه) مهندس شبكات محترف في ثلاث سنوات (هذا شعار الخطة الزمنية ومدتها ، ثم التقييم والمراجعة كل شهر ثم كل سنة ، ماذا أنجزت وفيما أخطأت وهل تحتاج الخطة لإعادة هيكلة وهكذا ... دعك من العشوائية وكن منظماً .

الكورس الأول :::

دعني أسألك سؤال أيها المبتدئ ما هي وحدة بناء الشبكة (شبكة الحاسب الآلي) ؟ [لا تستعجل أيها المتقدم في المستوى قليلاً فأنا سأتدرج حتى مستوى الخبراء ولكني أراعي المبتدئين فلا تمل وإنتظر وسوف تستفيد]

تمام صحيح : الكمبيوتر (الحاسب الآلي) هو وحدة بناء الشبكة

إذن لابد لك أن تتعلم استخدام الحاسب الآلي الويندوز والبرامج الأساسية الأوفيس مثلاً ، وهذا يمكن تغطيته بكورس الـ **ICDL** (International Computer Driving License) الرخصة الدولية لقيادة الحاسب الآلي .

ICDL International Computer Driving Licence

وأنا أعتقد أن أغلبكم يعرف مثل هذه المعلومات وإلا ما كانت وصلته تلك المجلة ولا قرأ هذا المقال ...

لكن ما لابد لك أن تتعلمه وهو شيء هام جداً في طريقك هو صيانة الحاسب الآلي ، مثل مكوناته وأنواعها وتركيبه وتحميل نظام التشغيل عليه وأنواع نظم التشغيل مثل الويندوز

وكذلك تركيب البرامج من أول الأوفيس لغاية الجافا وإصلاح المشاكل في الهاردوير أي الصيانة أو السوفت وير أي البرامج و... إلخ

والكورس الذي يغطي هذه الجزئية وبشكل ممتاز هو كورس A+ كورس الصيانة المتقدم .

إذن البداية بكورس A+ وهذا الكورس مقدم من خلال شركة CompTIA !!! كومبتيا

ليس الآن وقت التفاصيل أعرف أن همتك العالية تجعلك الآن تريد أن تعرف معلومات كثيرة عن هذا الكورس مثل مدته والمناهج الخاص به وأين يدرس وتكلفته واختباراته ومن هي CompTIA هذه ، لكن إتفقنا ألا تستعجل خلينا نتفق على نقطتين

الأولى : أننا مازلنا في الحلقة الأولى من السلسلة وهناك حلقات ستكون مخصصة للكلام عن كل كورس سأذكره بالتفصيل وخصوصاً الشركة المقدمة لهذا الكورس ...

الثانية : أننا سنتبع أسلوب التأصيل ثم التفصيل بمعني أننا سنذكر الخطة التي سنسير عليها بالكامل ملخصة ، خطتي خلال الثلاث سنوات القادمة ، ثم نبدأ بشرحها تفصيلياً والله الموفق ، نسألكم الدعاء ...

الكورس الثاني :::

بعد إتقانك لأساسيات الصيانة ، لابد أن تتعلم أساسيات هذا العلم ، علم الشبكات ... فالشبكات والله العظيم ولا أكون مبالغ علم عظيم من علوم هذا العصر ، علم يحتاج لأعمار فيه تفنى لكن الله الموفق ، نسأل الله أن يبارك لنا في أعمارنا وأن يعمرها بما ينفعنا في الدنيا والآخرة

لذلك البداية لابد وأن تكون من شركة أو منظمة حيادية غير منحازة لمنتجها على حساب المنتجات الأخرى من الشركات المنافسة ، وتلك المنظمة هي نفسها CompTIA فهي جهة غير هادفة للربح وليس لها أي منتج تنحاز له سنوضح ذلك لاحقاً .

فمثلاً Cisco سيسكو كل كورساتها تطبق المفاهيم العلمية للشبكات على أجهزتها وفقط ، ليل نهار تتحدث عن التكنولوجيا الخاصة بها

وأيضاً Microsoft مايكروسوفت كذلك ليل نهار تتحدث عن التكنولوجيا الخاصة بها يعني بعد كورس A+ بأي كورس أبدأ ؟ إبدأ بـ Network+

شركة CompTIA تقدم كورس في مبادئ وأساسيات الشبكات يسمى Network+ تتكلم فيه عن الشبكات كعلم وليس كشرح لآلية عمل منتج معين .

لكن ما تكلفتها ومدتها اتفقنا أننا سنكتب مقالات خاصة عن كل كورس من هذه الكورسات ، لكن عموماً هذه الكورسات غير مكلفة ووقتها ليس بالطويل .

إلى اللقاء في الحلقة القادمة

تقرأون في هذه الحلقة :::

مهندس شبكات محترف في ثلاث سنوات

الكورس الأول : A+

الكورس الثاني : Network+

تقرأون في الحلقة القادمة :::

ما هي الكورسات التالية ؟؟؟

لا تيأس من روح الله ...

لابد وأن تقوي نفسك في اللغة الإنجليزية ...

الآن تستطيع أن تعمل في مجال الـ IT ...

CCNP, CCNA, Network+ ...

تعرف على تقنية الـ Virtualization

بقلم : أيمن النعيمي

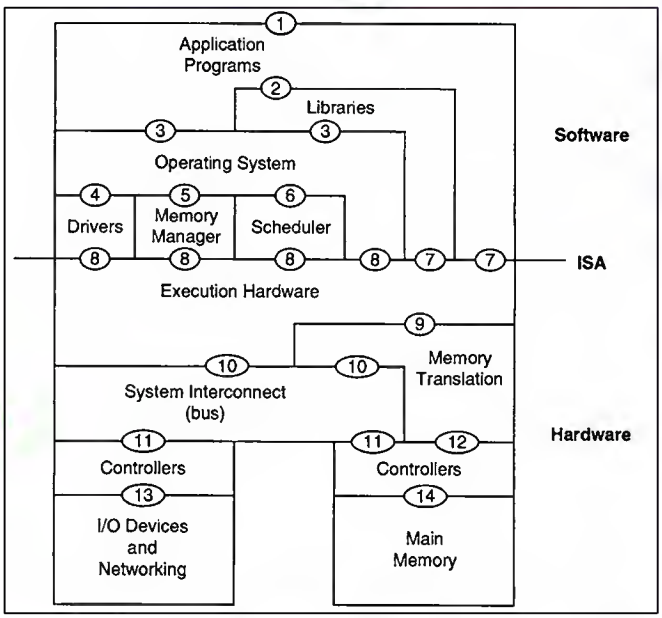
Virtualization أو التمثيل الأفتراضي تلك الكلمة التى شدت العالم بأسره إليه وكثيرة هي الأسئلة التى طرحت حولها ولم تجد لها أجابة وهذا ماسوف أقدمه لكم في هذا المقال البسيط الذي سوف أستعرض فيه كيفية وأسباب نشوء هذه التقنية بالأضافة إلى الفوائد التى تحققها هذه التقنية

مقدمة

قد يعتقد البعض أن هذه التقنية هي حديث العهد نتيجة التطور الكبير الذي نراه كل يوم في أجهزة الكمبيوتر أو العتاد المكون لها والحقيقة غير ذلك أبدا لأن بدايات هذه التقنية قديمة جدا وتعود إلى عام 1960 وأول من طورها كانت شركة IBM أو International Business Machines فكما هو معروف ان أجهزة الكمبيوتر في ذلك العصر وأخص بالذكر جهاز IBM 7044 (M44) كانت تقوم بعملية معالجة واحدة كل مرة والذي أنعكس سلبا على مقدرة المعالجات للعمل وخصوصا أن تطوير قوة المعالجات لم يكن بالأمر الصعب والتى كانت سبب في ولادة تقنية التمثيل الأفتراضي التى أتاحت أستخدام قوة المعالج من قبل عدة أشخاص من خلال تقسيمه إلى عدة أجهزة وهمية يتم التحكم بها من خلال أجهزة مخصصة أو Client وبالتالي أتاح لهم أمكانية تشغيل أكثر من تطبيق في تفس الوقت ,وقد واجهت هذه التقنية في حينها مشاكل كثيرة مثل عدم تمكين العملاء من تشغيل البرامج الغير أمنة untrusted لان أدائها يمكن أن ينعكس سلبا على النواة بشكل عام بالأضافة إلى عدم مقدرة كل عميل القيام بأي عملية تحديث أوترقية للنظام الخاص به وآخيرا لم يكن هناك أمكانية للتحكم بتقسيم العتاد بشكل منصف بين أجهزة العملاء .

كيف تعمل هذه التقنية

يحتاج منك لفهم كيف تعمل هذه التقنية الكثير من الوقت والكتب لكن سوف أقدم لمحة بسيطة عن مبدأ عملها لذا دعوني أولا أقدم لك هذا المخطط الذي يوضح الطبقات الموجودة في الكمبيوتر



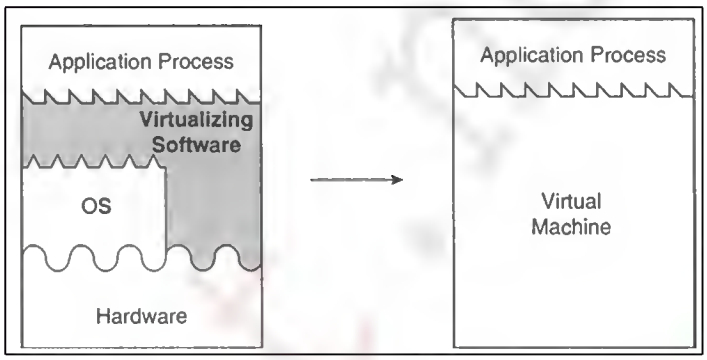
فكما هو واضح أن للكمبيوتر عدة طبقات

الطبقة الأولى خاصة بي البرامج او Software وهي بحد ذاتها مقسمة لعدة طبقات ونستطيع أن نشاهد أن هناك برامج تعمل من خلال الأتصال بالهاردوير بشكل مباشر وهناك من يتصل بطبقة المكتبات التى تخص نظام التشغيل والخ...

الطبقة الثانية Instruction Set Architecture أو ISA وهي الطبقة التى تفصل طبقة الهاردوير عن السوفت وير وهي النقطة التى بنى فيها المطورون أول أفكار تقنية التمثيل الأفتراضي

الطبقة الثالثة وهي طبقة الهاردوير وهي توضح المدخلات والمخرجات الخاصة بالكمبيوتر

فمن خلال طبقة ISA قام المطورون بتطوير تقنية التمثيل الأفتراضي لتتمثل لنا بهذه التقسيمة البسيطة الموضحة بالصورة القادمة والتى تتيح أمكانية التحكم في موارد الهاردوير الموجودة من خلال نظام تشغيل خاص بها يدعى hypervisor او virtual machine monitor (NMM) والتى بدورها تسمح لنا بتنصيب أكثر من نظام تشغيل ومارقبتها وأعدادها طبعا



وكما ذكرت أن الموضوع يحتاج الكثير من الشروحات والتحليلات ولأني أردت أن يكون الموضوع مفهوم لجميع الفئات وأنصح أي شخص يريد أن يعرف أكثر عن آلية العمل أن يقرأ كتاب Virtual Machine الذي كتب بواسطة James E.Smith & Ravi Nair

ماهي الفائدة التى نحققها

وهو السؤال الأهم في موضوعنا ما الذي توفره لي هذه التقنية ولسنتعرضها بالتسلسل التالي:

توفير المال : من أكثر الحقائق غرابة أن أغلب أجهزة الكمبيوتر الموجودة في عصرنا لاتستخدم أكثر من 10% من قدرتها وطاقتها وطبعا هذه الحقيقة ترجعنا إلى عام 1960 وهي لماذا لأ أستفيد من طاقة المعالج بشكل كامل وفي نفس الوقت أوفر على نفسي المال لشراء كمبيوتر آخر يقوم بأعمال آخرى

توفير الوقت : من خلال نظام تحكم واحد سوف تستطيع الوصول إلى كل الاجهزة والسيرفرات الموجودة لديك وبالتالي سرعة في أكتشاف الأخطاء وإصلاحها زد على ذلك سرعة القيام بعمليات الصيانة الدورية والتى تشمل أمور مثل backup, archiving and recovery فمن قبل كان يتطلب منك تنصيب ويندوز سيرفر وأعداده حوالي الثلاث ساعات لكن مع التمثيل الأفتراضي لن يستغرق معك الأمر أكثر من ثانيتان من خلال القيام بعمل صورة لنظام التشغيل .

توفير الطاقة : أن التوفير التى تقدمها لنا تقنية التمثيل الأفتراضي في الطاقة كافية لأن تكون هي الفائدة الوحيدة لها فمن خلال تقليل عدد السيرفرات التى تعمل إلى أكثر من النصف سنجد ان الطاقة التى تخصص لها قد نقصت بمعدلات كبيرة والتى أكدها مستخدمي برنامج VMWare الذين صرحوا بتوفير حوالي 60% من الطاقة المستخدمة

توفير في الشبكات : فكما هو معروف أن الربط بين السيرفرات الحقيقية يحتاج منك سويتشات وروترات تقوم بهذه العملية لكن مع تقنية التمثيل الأفتراضي سوف تقوم بهذه العملية بشكل مجاني وبأداء وسرعة قد تكون أفضل وأأمن من الشبكة العادية.

سهولة التحكم : فمن خلال جهاز واحد سوف تستطيع الوصول لجميع الأجهزة أو Desktop الخاص بكل كمبيوتربالأضافة إلى أمكانية مراقبة أداء وعمل كل الأجهزة من شاشة مراقبة واحدة تعطيك كل التفاصيل المطلوبة

الأمان والحماية : فمن خلال الأجهزة الوهمية الموجودة تستطيع أن تقوم بتجربة بعض البرامج الغير أمنة والتأكد من خلوها من أي فايروسات أو ديدان خبيثة وبالتالي حماية سيرفراتك منها

أمكانية تنصيب وأستخدام عدة أنظمة تشغيل على جهاز واحد مثل ويندوز لينوكس أبل دوس .

هذه كانت أهم الفوائد التى تحققها لنا تقنية التمثيل الأفترضي وهناك أيضا المزيد من الفوائد التى تختلف بحسب أنظمة التشغيل التى تقوم بأستخدامها وهذه لائحة بأهم الشركات المطورة لهذه التقنية

Xen 3.0: أحد الأنظمة المفتوحة المصدر والتى تحوي على حوالي 50.000 سطر من الاوامر وهي تعمل على كل من معالجات Intel or AMD x86 and 64-bit

VMWare: وهي الأشهر في هذا المجال والأكثر تحميلا بين باقي الأنظمة وخصوصا بعدما اتاحة برامجها للتحميل بشكل مجاني وهي تملك عدة برامج فمنها من يعمل من خلال أنظمة التشغيل نفسها مثل VMWare-Server أو Player بالأضافة إلى وجود نظام تشغيل يدعى VMWare ESX Server خاص بأدارة عملية التمثيل الأفتراضي أو كما قمنا بتعريفها من قبل بي Hypervisor

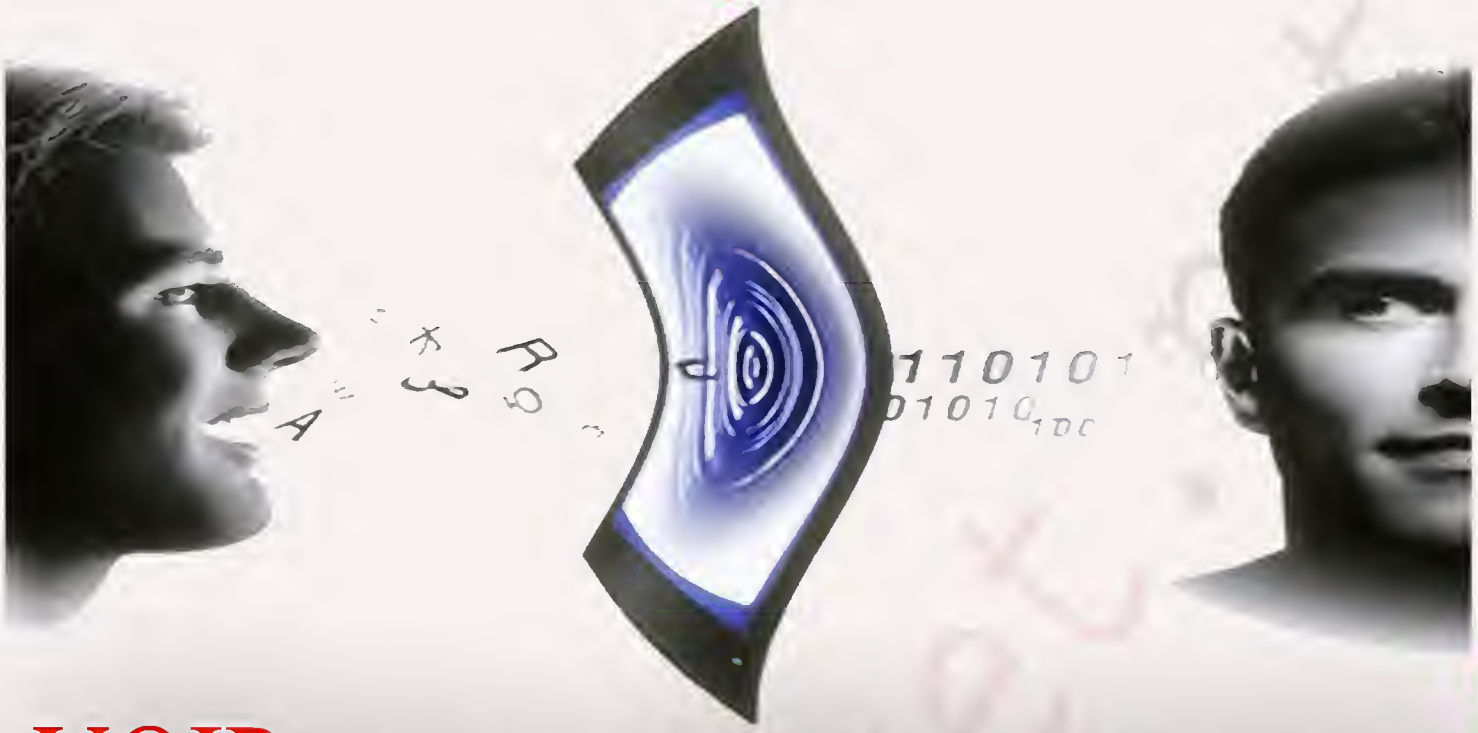
Microsoft Hyper-v : وهي تعرف بي Windows Server 2008 Hyper-V وهو النظام المطور من خلال مايكروسوفت والذي أصبح جزء من ويندوز سيرفر 2008

Sun VirtualBox : أيضا نظام تشغيل مفتوح المصدر مشابه لي XEN

Citrix XenServer : نظام مبني على Xen Hypervisor وهو مجاني أيضا

Virtual Iron
IBM Virtualization Engine Platform
SWSoft Virtuozzo
OpenVZ
Linux-VServer
QEMU

هذه كانت لمحة بسيطة عن هذه التقنية الرائعة وأن كنت لم أغطي كل شيء عنها في هذا المقال فهي أكبر بكثير من أن يتم تغطيتها بمقال واحد والذي سوف أتركه لكم في العدد القادم



كيف تقوم بتأسيس شبكة فويس من الصفر (VOIP)

بقلم أحمد الشحات

سوف أحاول في هذا الموضوع شرح طريقة أعداد شبكة فويس من الصفر لذا سوف يكون الموضوع مقسم لعدة أجزاء وسوف يتم نشر باقي الأجزاء في الأعداد القادمة آن شاء الله وسوف يقتصر هذا الموضوع على مقدمة حول البروتوكول وتوضيح فوائد أستخدامه .

مقدمة

Viop هو اختصال لكلمة Voice Over Internet Protocol وهي عبارة عن نقل الصوت عبر الشبكة الى تستخدم البروتوكول IP وهذا يشمل النقل عبر الأنترنت او عبر الشبكات العادية ويعود تاريخ هذه الفكرة إلى عام 1995 بواسطة بعض المستخدمين العاديين للانترنت والتى تطورت لتشمل نقل الصوت والصورة ولتمكين هذه الخدمة نحتاج إلى أجهزة تلفون خاصة تدعى بي IP Telephony والتى سوف يتم التطرق اليها في الأجزاء القادمة .

طريقة النقل

فى نقل الصوت عبر الشبكة يتم تحويل الصوت من analog الى رقمي ويتم تقسيم الاشارة الى حزم صغيرة يسهل نقلها ويتم النقل فى عدة مسارت لضمان سرعة الوصول وعند وصولها الى جهة الوصول يتم تجميعها مرة اخرى بعكس الاشارت ال analog القديمة حيث أنها تاخذ مسارا واحدا فقط للوصول الى المستمع واذا كان المستمع فى جهة الوصل من النوع analog فيتم تحويلها مرة أخرى الى analog لكي يستطيع الجهاز فهمها

فوائد أستخدام VOIP

عندما بدأ موضوع نقل الصوت عبر الشبكة VOIP المعظم قالو ما الفائدة لو ارسلنا الصوت عبر الشبكة والفائدة الوحيدة ستكون هي توفير ثمن الكابلات فقط ولكن عند البحث فى فوائد نقل الصوت عبر الشبكة سوف نجد فوائد كثيرة سوف نستعرضها الآن

تقليل ثمن المكالمات

حيث أن المستخدمين للشبكة يستطيعون عمل اى عدد من المكالمات فيما بينهم مجانا ليس هذا فقط بل أن هناك ستكون Dial Plan دائمة يستطيع فيها المستخدمون الاتصال فيما بينهم مجانا ومن خلال تحويلة مكونة من أربعة أرقام مثلا وفي جميع أنحاء العالم لنفس الشبكة فمثلا لو كان لديك شركة فى السعودية واحد فروعها فى مصر والفرع الاخر فى سوريا وهكذا فان الموظفين سيتصلون مجانا فيما بينهم وبتحويلة داخلية فقط ولا داعي للاتصال بالارقام الدولية ومفاتيح الخطوط الدولية

تقليل تكلفة تمديد الكابلات بطريقة رهيبة

حيث أنه النقل يتم عبر كابلات الداتا فلن نستخدم كابلات الفويس وتخيل لو مشروعك يقع بين عدة مدن وطبعا تستطيع أن تتخيل التوفير الذي تم من عدم استخدام كابلات الفويس

سلاسة وانسيابية الشبكة

كما قلنا ان النقل يتم عبر شبكة الداتا التي هي اصلا قد قامت بتوصيل المكاتب والمستخدمين من قبل فأن شبكة الصوت تلقائيا ترث تلك الخصائص عن شبكة الداتا وتصل لنفس المدى الذي تصله شبكة الداتا بدون برمجة اضافية او تكلفة اضافية ليس هذا فقط بل أن هناك تحكم مركزي بكل الاجهزة المتصلة بالشبكة

التنقل بالتليفون بسهولة

الأن اى موظف يستطيع حمل تليفونه الى المكتب المقابل او الطابق الاخر وبمجرد توصيله بالشبكة سيأخذ نفس الاعدادات القديمة وبدون برمجة اضافية

كما انه لو كان هناك اتصال VPN فأن الموظف يستطيع مل تليفونه معه الى المنزل وياخذ نفس الاعدادات

Ip Soft Phons

يعتبر برنامج سوفت فون مثال رائع عن طريقة اندماج شبكة الداتا مع الفويس فالآن بمجرد وصل سماعة صغير وميكرفون بالكمبيوتر الخاص بك تستطيع ان تعامل مع الشبكة كان لديك تليفون حقيقي كمان ان برنامج سوفت فون الآن يتكامل مع التطبيقات الأخرى مثل الماسينجر وجهات الاتصال والايميل

توحيد الرسائل

الأن تستطيع استقبال جميع الرسائل فى صندوق بريد واحد سواء كانت فاكس او رسالة صوتية او ايميل

زيادة الإنتاجية

توجد ميزة فى VOIP وهي انك تستطيع أن تجعل أكثر من تليفون يرن قبل ذهاب الرسالة الى الفويس ميل

ولذلك في حالة عدم وجود الموظف سيرد موظف أخر بديلا عنه ويقوم بإنهاء المهمة بدلا من الموظف الهارب

تكامل أنواع مختلفة من الأجهزة

الآن تستطيع العمل مع أجهزة مختلفة فى الشبكة الواحدة ممكن يمكنك من اختيار الأفضل لشبكتك بدون التعقيد بمصنع وحيد

وفي العدد القادم سنتكلم عن شكل وتركيب شبكة الفويس ان شاء الله .

دليلك نحو شهادات جونيبر

أعداد: أيمن النعيمي

تملك جونيبر عدد كبير من الشهادات العلمية المختلفة والتى تغطي كل منتجاتها في الشبكات وأن كان البعض منها تجاري بسبب تكرر المواضيع فيها لذا سوف احاول في هذا الموضوع القاء الضوء على أهم الشهادة الموجودة وأرقام الأمتحانات الخاصة بها

قبل أن نبدأ أريد أن ألفت أنتباهك إلى شيء مهم وهو فهمك لمنتجات جونيبر يساعدك في أختيار الشهادة الأفضل للدراسة وقد تم شرح منتجات جونيبر في العدد السابق ولنبدأ

JNCIA JNCIS

Juniper Networks Technical Certification Program (JNTCP)
Firewall/VPN Track

JNCIA JNCIS JNCIE

Juniper Networks Technical Certification Program (JNTCP)
Enterprise Routing Track

JNCIA JNCIS JNCIP JNCIE

Juniper Networks Technical Certification Program (JNTCP)
M/T-series Routers Track

E Series Track

هذه الشهادة خاصة بالتعامل مع أجهزة جونيبر من الـ Series E وفيها 3مستويات

JNCIA JNCIS JNCIP

Juniper Networks Technical Certification Program (JNTCP)
E-Series Routers Track

وهي تتحدث عن المواضيع التالية virtual routers, BRAS, routed & bridged 1483, PPP over A™, PPP over Ethernet, dynamic configuration mode, L2TP, policy management

وهذه لائحة بأرقام الأمتحانات ومتطلباتها

E Series	رقم الأمتحان	الشهادات المطلوبة
JNCIA-E	JNO-120	لايوجد
JNCIS-E	JNO-130	لايوجد
JNCIP-E	CERT-JNCIP-E	JNCIS-E

Firewall/VPN Track

لهذه الشهادة مستويان فقط المبتدأ Associate والمختص Specialist وكما هو موضح بالصورة التالية

JNCIA JNCIS

Juniper Networks Technical Certification Program (JNTCP)
Firewall/VPN Track

وهي تتحدث عن المواضيع التالية VPNs, Network Management, Troubleshooting with Debug & Snoop, Traffic Management, Virtual Systems, NSRP, Dynamic Routing/Routing over VPNs, Attack Prevention, Multicast وهذه أرقام الامتحانات ومتطلباتها

Firewall/VPN	رقم الأمتحان	الشهادات المطلوبة
JNCIA-FWV	JNO-522	لايوجد
JNCIS-FWV	JNO-532	لايوجد

هذه كانت أهم الشهادات برئي الشخصي وليس كلها لان في جونيبر هناك المزيد من الأمتحانات وهذه لائحة ببباقي الأمتحانات

Intrusion Detection & Prevention (IDP) Track
SSL Track
DX Track
WX Track
Unified Access Control (UAC) Track

وعلى هذا الرابط تستطيع إيجاد تفاصيل أكثر عن الشهادات
www.juniper.net/us/en/training/certification

Enterprise Routing Track

شهادة الراوتينغ وهي تتألف من 3مستويات المبتدأ Associate والمختص Specialist والخبير Expert

JNCIA JNCIS JNCIE

Juniper Networks Technical Certification Program (JNTCP)
Enterprise Routing Track

وهي تتحدث عن كيفية أدارة الروتر والبروتوكولات الخاصة بالروتينغ مثل OSPF,BGP, RIP,NAT,VPN وأرقام الأمتحان على الشكل التالي

M&T Series	رقم الأمتحان	الشهادات المطلوبة
JNCIA-M	JNO-201	لايوجد
JNCIS-M	JNO-303	لايوجد
JNCIP-M	CERT-JNCIP-M	JNCIS-M
JNCIE-M	CERT-JNCIE-M	JNCIP-M

Enterprise Switching Track

للسويتش هناك شهادة واحدة فقط وهي JN0-400 وهي بمرتبة مبتدأ Associate

Junos Security Track

لهذه الشهادة أمتحان واحد أيضا وهو JN0-331 هو بمرتبة Specialist ولكي تستطيع أن تتقدم لهذا الأمتحان يتوجب عليك ان تحصل على أحد هذه الشهادات JNCIA-JUNOS, or JNCIA-ER, or JNCIA-M

وهي تتحدث عن المواضيع التالية Introduction to SRX-series, Zones, SCREEN Options, Security Policies, NAT, IPSec VPNs, HA Clustering, Intro to IDP, Firewall User Authentication

M Series & T Series Track

هذه الشهادة خاصة بالتعامل مع أجهزة جونيبر من الـ Series M&T ولها أربع مستويات كما هو واضح من الصورة

JNCIA JNCIS JNCIP JNCIE

Juniper Networks Technical Certification Program (JNTCP)
M/T-series Routers Track

وفيها مواضيع مكررة مع أمتحانات الراوتينغ(ER) وهي بشكل عام تتحدث عن BGP, OSPF, IS-IS, and RIP, routing policy, firewall filters, CoS, MPLS, VPNs, IPv6, and multicast

وهذه لائحة بأرقام الأمتحانات ومتطلباتها

M&T Series	رقم الأمتحان	الشهادات المطلوبة
JNCIA-M	JNO-201	لايوجد
JNCIS-M	JNO-303	لايوجد
JNCIP-M	CERT-JNCIP-M	JNCIS-M
JNCIE-M	CERT-JNCIE-M	JNCIP-M

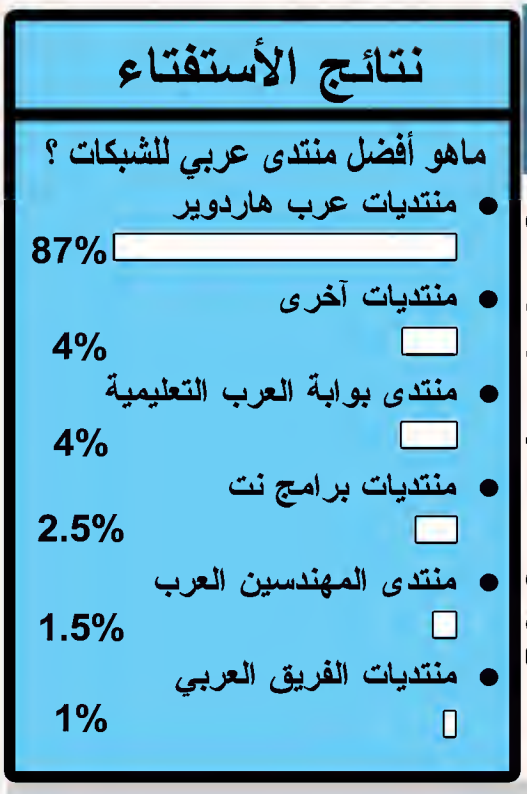
نتائج الأستفتاء الشهري

مع 135مصوت تم اغلاق الاستفتاء الآخير على المدونة وطبعا العنوان ما هو أفضل منتدى عربي للشبكات وصراحة نتائج التصويت كانت مخالفة بعض الشيء لتوقعاتي ,فقد توقعت أن يكون عرب هردوير هو الرابح الأكبر لكن ليس بهذه النسبة العالية وهذا يدل على الثقة الكبيرة التى نالها هذا المنتدى في عالم الشبكات وسبب نجاح منتديات عرب هاردوير في عالم الشبكات برائي يعود إلى سببين

ا-السبب الأول وهو سبب نجاح أي منتدى في العالم هو الأعضاء نفسهم فبوجود نخبة كبيرة من الأعضاء تقوم بتقديم المساعدة وأرشاد باقي الأعضاء إلى أمور الشبكات وكورساتها وطريقة حل مشاكلها كان من أقوى الأسباب التى أدت إلى نجاح المنتدى

ب-الأساتذة والمشرفين الموجودين في المنتدى والذي لهم دور فعال في نشر العلم وأخص منهم الأستاذ محمد سمير والأستاذ لومارك وأحمد سرحان وأحمد جودة وطبعا الأستاذ ياسر رمزي بالأضافة إلى باقة كبيرة من الأساتذة .

والكلمة الآخيرة التى احب أن أضيفها هي أن منتديات عرب هاردوير قد حولت عالم الشبكات إلى تاريخان تاريخ الشبكات قبل عرب هاردوير وتاريخ الشبكات بعد عرب هاردوير ونيابة عني أشكر جميع القائمين على المنتدى من أداريين مشرفين مؤسسين والشكر الأكبر للأعضاء التى تساهم فيه دائما وبشكل آيجابي



أنواع كوابل الإيثرنت وكيفية أختيار الكبل المناسب

بقلم أيمن النعيمي

لنتفق أولا على أن كوابل الإيثرنت ليست متشابها وهي تختلف بحسب قدرة الكبل على نقل البيانات فيها ونستطيع أن نفرق بينها من خلال آما النظر أو من خلال قراءة ماكتب عليها لكننا سوف نقع في حيرة من أمرنا لان هذا النوع من الكوابل له الكثير من الأنواع ولفهمها يجب أن نعلم أن للكوابل تصنيفات عالمية أو مايعرف بي Categories وقد صدر منها حتى الآن 7تصنيفات وفهمك لهذه التصنيفات يعطيك القدرة على أختيار الكبل المناسب للعمل والذي يتناسب مع متطلبات العمل لديك وطبعا هذه التصنيفات ليست كلها لتقنية الإيثرنت بل يوجد أستخدامات آخرى لذا لن اكتفي بعرض تصنيفات الأيثرنت فقط بل سوف أقوم بعرض كل التصنيفات للفائدة العامة مع الأشارة إلى أستخدام كل نوع منها

CAT 1

وهي أختصار لكلمة Categories وهو أول وأقدم تصنيف وغير متعلق بتقنية الأيثرنت وهو يستخدم عادة في كوابل الهاتف وخطوط الـ ISDN

CAT 2

التصنيف الثاني هو أيضا غير متعلق بتقنية الأيثرنت وأستخدامه محصور في ميغا بت في الثانية 4وتصل سرعته القصوى إلى Token Ring شبكات الـ 1MHz وبتردد

CAT 3

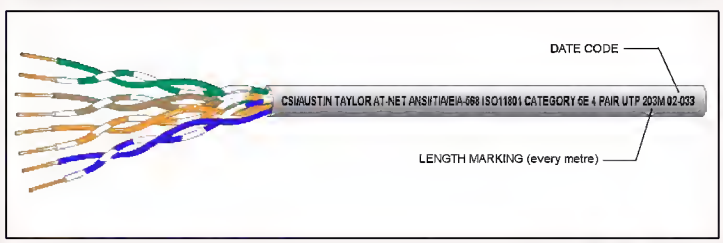
وهو أول كوابل الإيثرنت وسرعته تصل إلى 10ميغا بت وبدأ استخدامه في بداية التسعينات ولكن توقف أستخدامه في الشبكات بعد ظهور CAT 5ولينحصر أستخدامه الآن في الأتصالات أو عبر مايعرف بي VoIP telephone وبتردد وصل إلى 16 MHz وهذه صورة توضيحية للكابل

CAT 4

هذا التصنيف أيضا يتبع شبكات الـ Token Ringوهو عبارة عن أربع أزواج من الأسلاك وتصل سرعة النقل إلى 16ميغا بت وبتردد 20 MHz

CAT 5

قام هذه النوع من الكوابل بأحداث نقله نوعية في الشبكات بتوفيره سرعة كبيرة مقارنة بأقرانه السابقين والتى وصلت إلى 100ميغا بت وهو يعمل مع تقنية الإيثرنت ويصلح لكي يعمل مع تقنية نقل الصوت والـTokenRing والـ ATM



CAT 5E

كما واضح من الأسم يعد هذا التصنيف شكل متقدم عن الـ CAT 5ومايميزه هو دعمه لي Gigabyte Ethernetوتصل سرعته إلى 125ميغا بت كحد أقصى

CAT 6

هو التصنيف الرسمي لي Gigabyte Ethernet وسرعته تصل إلى ضعف سرعة CAT 5e اي حوالي 250- ميغا بت وهذه صورة توضيحية

CAT 6A

أيضا تصنيف مطور من السابق وبسعة نقل وصلت إلى الضعف لدعم الـ 10Gigabyte Ethernet أي حوالي 500ميغا بت

CAT 7

وهو التصنيف الرسمي لي 10Gigabyte Ethernet وبسرعة تجاوزت التصنيف السابق لتصل إلى 600ميغا بت وقد تم عزل كل زوج من الأسلاك عن الآخر بشكل كامل كما هو موضح بالصورة

CAT 7A

تصنيف مطور عن السابق لدعم السرعات التى تصل إلى 100Gigabyte Ethernet وبسرعة وصلت إلى 1000ميغا في الثانية

شهادة جديدة من سيسكو CCNA SP

أعلنت سيسكو بتاريخ 5-أيار/مايو عن طرح شهادة جديدة خاصة بي الـService Provider بمستوى مبتدأ Associate وليكتمل الهرم الخاص بهذه الشهادة وتحمل هذه الشهادة الرقم 640-760 وتحمل الأسم التالي Supporting Cisco Service Provider IP NGN Operations (SSPO) وهي تتحدث بشكل عام عن المبادئ الرئيسية في أعداد مخدمات الأنترنت بالأضافة إلى مقدمة عن IP NGN أو IP Next-Generation Network وهي طبعا الجيل الجديد من أجهزة سيسكو CRS
وهذه لائحة بمحتويات هذه الشهادة

Perform the network incident management process
Describe how a trouble ticket processes through the network operations center(NOC)
Identify key network incident metrics in a NOC incident report
Apply an incident management process
Perform incident management using basic tools and documentation
Close an incident ticket
Prioritize incident tickets according to standards
Escalate an incident ticket according to typical criteria
Create an RFC to implement a fix or workaround for an incident

Apply the problem management process
Apply the Information Technology Infrastructure Library (ITIL) problem management process to the task of managing networks
Distinguish between incident management and problem management, and determine the interactions that occur between them

Perform first-level network monitoring and troubleshooting
Use network management tools to monitor network status
Interpret device specific alarms and determine the severity of the alarm
Initiate troubleshooting procedures based on received alarms and/or log messages
Use network management tools to troubleshoot first-level network incidents
Use syslog functions, severity levels, syslog traps, and buffering
Use knowledge of IP fundamentals to determine the most likely cause of a network problem
Determine the most probable cause of a problem from standard output and SNMP traps
Utilize common structured troubleshooting approaches

Perform network configuration management
Backup configurations across standard NOC architectures
Interpret basic standard scripting commands used in automating network maintenance
Interpret basic UNIX cron job commands used in automating network maintenance
Use a network inventory management process

Implement network changes and change management
Accurately document a network
Utilize a network change implementation rollback
Implement a network change based on change documentation
Perform a network upgrade
Identify upgrade or downgrade issues and recommend corrective actions
Verify the usability and effectiveness of a network change

Apply the fundamental concepts of service level agreements (SLAs)
Identify the unique characteristics of different SLAs
Inform customers about SLA issues
Monitor service levels against the requirements of an SLA

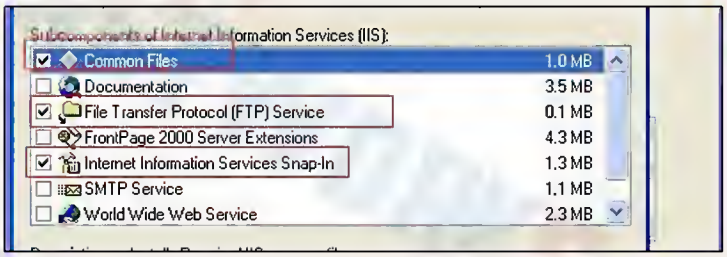
Describe basic IP technology in the Service Provider NOC
Describe the purpose and components of an IPv4 address
Describe the purpose of and components of IOS XR
Use IOS XR to perform basic router functions
Compare and contrast IPv4 to IPv6 addresse

كيفية تفعيل J-Web والحصول على كل مميزاته

عودة مره آخرى مع جونيبر وهذا المرة لكي نقوم بتفعيل J-web والتى من خلالها تستطيع أن تتحكم بالروتر أو السويتش من خلال واجهة رسومية تتيح لك أن تقوم بجميع الأعدادت اللازمة بالأضافة الى الكثير من أقسام المراقبة الخاصة بالأداء وهي طبعا مشابهة لعمل الـSDM الموجودة في أجهزة سيسكو.ولكي تتم عملية التشغيل يلزمنا j-web Package خاصة بكل أصدار من JUNos ويتم تحميلها أولا على الروتر وبعدها نقوم بتسطيبها على نظام التشغيل JUNos والشرح سوف يكون على النسخة الخاصة بالأصدار 9.0
وسوف يكون بمساعدة VMware +Olive من خلال عدة مراحل

المرحلة الأولى

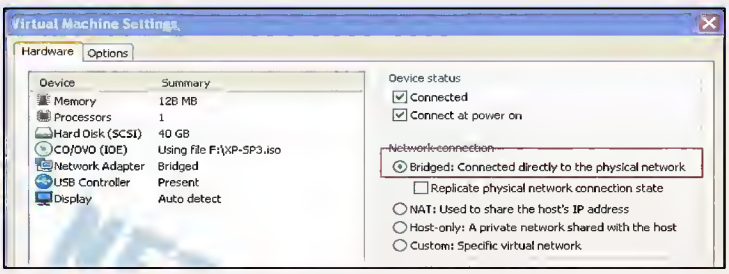
هي تثبيت سيرفر FTP على ويندوز أكس بي مثبت على VMWare والهدف منه تكوين سيرفر نستطيع من خلاله أن نسحب الباكيج الى داخل الروتر وطريقة تثبيته بسيطة جداأتبع الترتيب التالي–> Start control Panet –> Add/remove --> add/remove windows components -->Intenet Information Services IIS وبعدها قم بأختيار FTP Service كما هو موضح بالصورة



بعد الأنتهاء من التنصيب سوف يظهر مجلد جديد على السي أسمه Inetpub وبداخله ملف ftproot في هذا الملف قم بوضع الباكيج الخاصة بالJ-web وبعدها سوف أعطي كرت الشبكة الأعدادات التالية

IP 192.168.1.2
Mask 255.255.255.0
Gateway 192.168.1.1

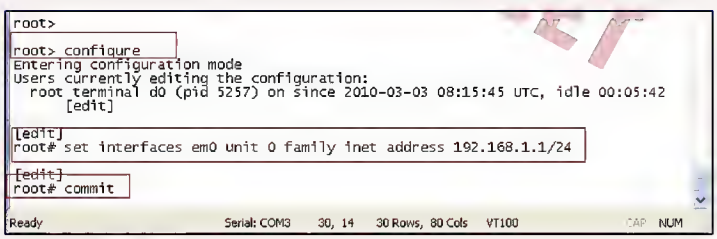
ولاننسى أن نضع أعدادت الشبكة الخاصة بي الVMwareكما هو موضح بالصورة حتى يكون هناك جسر بين الويندوز والروتر أي على الروتر وعلى الويندوز يجب أن نضع نفس الأعدادات



المرحلة الثانية

نتوجه الى روتر جونيبر ونقوم بأعطاء الانترفيس أيبي بالدخول على الـconfigure mode وتطبيق الأوامر التالية

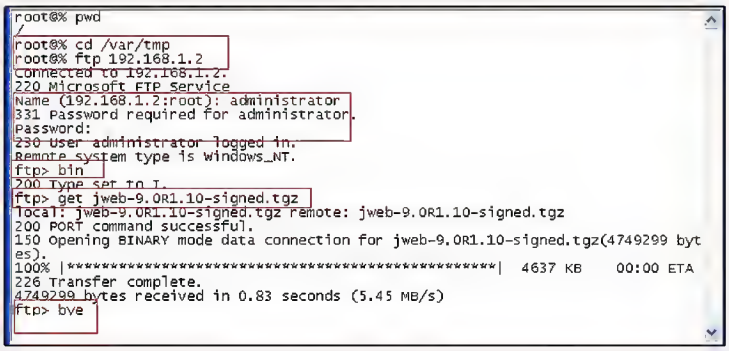
root# set interfaces em0 unit 0 family inet address 192.168.1.1/24
root# commit



وبعدها نقوم بالتأكد من وجود أتصال بين الويندوز والروت من خلال الأمر Ping

المرحلة الثالثة

هي الأتصال مع سيرفر الـ FTP وسحب الباكيج إلى داخل الروتر وذلك من خلال الأوامر الموضحة بالصورة التالية



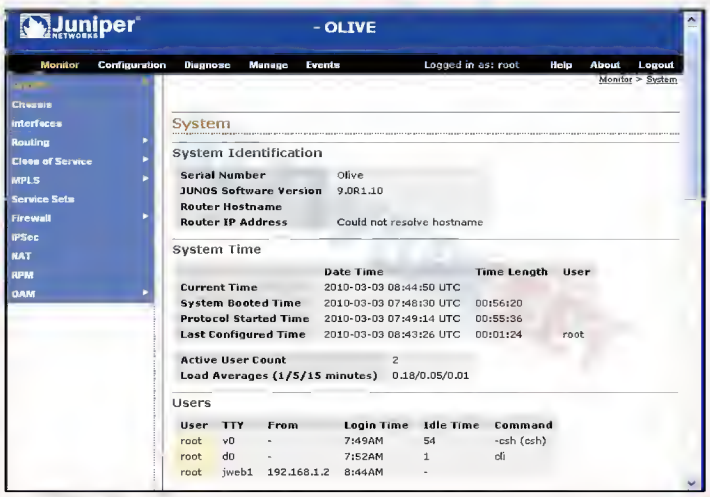
المرحلة الرابعة

تثبيت الباكيج على الروتر من خلال الأوامر التالية

بقي علينا أمر واحد وننتهي من الأعدادت وهي تفعيل الـ Http على البورت الذي سوف نقوم باللأتصال عليه من الويندوز وذلك من خلال الأمر التالي:

root# set system services web-management http interface em0.0
root# commit

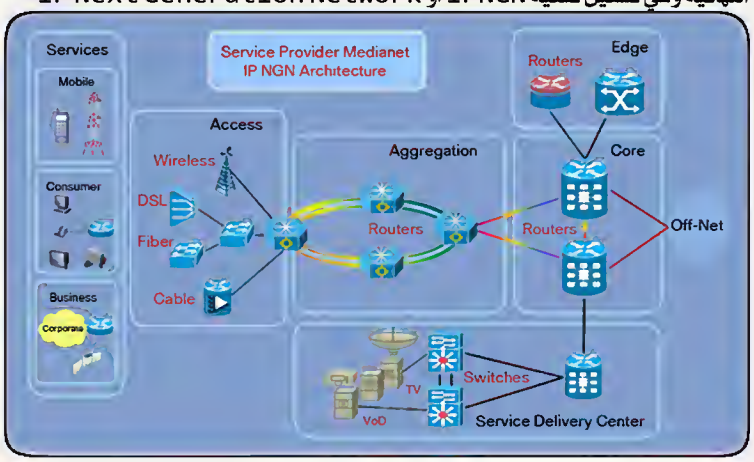
نذهب الآن الى الويندوز ونقوم بفتح صفحة أنترنت ونكتب فيها الأيبي الخاص بالروتر والنتيجة سوف تكون
"أهلا وسهلا بك في عالم جونيبر"



كيف تستغل وقتك في تعلم الشبكات

قد يمر على بعض الأشخاص أوقات يريد فيها أن يرفه عن نفسه ويبتعد قليلا عن الدراسة والقراءة على الكمبيوتر كما يحدث معي أحيانا لذا ألجا دائما إلى أن ألعب لعبة الـ Solitaire أو أتجه إلى موقع ياهو وألعب الشطرنج وقد تركت هذه الألعاب منذ تعرفت على ألعاب سيسكو وخصوصا لعبة الشبكات الأستراتيجية myPlanNet

فكرة اللعبة تبدأ مع عام 1990 من مدينة صغيرة لايوجد فيها أي نوع من الأتصالات لا تلفونات ولاكابل تلفزيون وطبعا لايوجد أنترنت وهي المهمات التى يجب عليك القيام فيها ففي بداية اللعبة يتاح لك أن تختار أما البدأ في تمديد المدينة بالتلفونات أو الوايرليس أو الايثرنت وطبعا هناك مراحل كثيرة تدخل في اللعبة والهدف منها هو أن تصل إلى المرحلة النهائية وهي تشغيل تقنية IPNGN أو IP Next Generation Network



وعندما تبدأ اللعب سوف تكتشف أهميتها فهي تعلمك كيفية بناء أستراتيجة شبكات من الصفر وأن كنت لم أتعلم اللعبة بشكل كامل فلي فيها 3 أيام فقط ولكن أستطعت أن أفهم فيها أشياء كثيرة واهم شيء التسلسل الذي يجب أتباعه في بناء الشبكة والكثير من الأشياء لذا أذا كان لديك أحيانا وقت فارغ فأنا أنصحك بتجربة هذه اللعبة بغض النظر عن المقولة بأن الألعاب للصغار فقط لتحميل اللعبة توجه إلى موقع سيسكو

http://www.cisco.com/web/solutions/sp/myplannet/index.html

ولمزيد حول اللعبة توجه إلى صفحت اللعبة على الـ FaceBook

http://www.facebook.com/pages/Cisco-myPlanNet/153538644090

كيف تقوم بعمل أختصار لجميع أوامر سيسكو

أحد الأشياء التى أجدها في سيسكو مميزة وتساعد كثيرا في كتابة الأوامر وتسريع العمل هو الأمر Alies يقدم هذا الأمر الكثير من المساعدة في أختصار الوقت في كتابة بعض الأوامر التى تحتاجها بشكل مستمر من خلال عمل أختصار له على شكل حرف أو حرفين وهو يقسم إلى ثلاثة أقسام رئيسية

القسم الأول خاص بالأوامر التى تكتب في الـPrivilegedMode وصيغة الأمر تكون على الشكل التالي

Alias exec

القسم الثاني خاص بالأوامر التى تكتب في الـGlobal Configuration Mode وصيغة الأمر تكون على الشكل التالي

Alias configure

القسم الثالث خاص بالأوامر التى تكتب في الـInterface Configuration Mode وصيغة الأمر تكون على الشكل التالي

Alias interface

وهذه بعض الأمثلة لتوضيح طريقة كتابة الأوامر في كل قسم

```
Router(config)#alias exec a show ip int br | exclu unass
Router(config)#alias exec sr show ip route
Router(config)#alias exec acl show access-lists
Router(config)#alias exec srint show running-config interface
```

وكما تشاهدون بعد كتابة الأمر alias exec أقوم بكتابة الحرف الذي أريده لكي يكون أختصارا للأمر show ip int br |exclu unass وطبعا قمت بأختيار الحرف a لتنفيذ الأمر ونفس الشيء مع باقي الأوامر

```
Router(config)#alias configure in interface fastethernet 0/0
Router(config)#alias configure eigrp router eigrp 10
Router(config)# alias interface x1 switchport mode access
Router(config)# alias interface x2 switchport port security
Router(config)# alias interface ns no shutdown
```

هذه كانت بعض الأمثلة التوضيحية وتستطيع أن تقوم بتجهيز أختصارات لاي أمر تحتاجه بشكل مستمر أضف على ذلك أن سيسكو قد قامت بأضافة بعض الأختصارات الجاهزة والتى تستطيع أستخدامه مباشرة وهذه أمثلة عليها

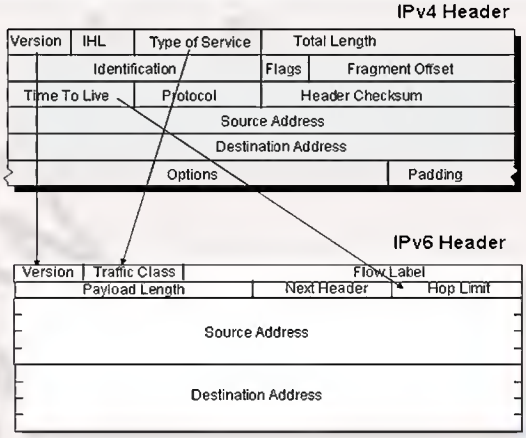
```
p stands for ping
h stands for help
lo stands for logout
u and un stand for undebug
wr stand for copy start run
w stands for where
```

كلمة آخيرة لهذا الأمر الكثير من الأقسام ووالتى ذكرتها تعتبر هي الأساسية وأكثر أستفادة يحققها لك هذا الأمر برائي هو الجزء المتعلق بأوامر الـ Show لانها من أكثر الأوامر التى نقوم بأستخدامها كما يعد أستخدام أمر Alias من النصائح التى توجه للأشخاص الذين يريدون الدخول إلى أمتحان العملي الخاص بي شهادة CCIE من اجل تسريع العمل

مقارنة بين IPv4 و IPv6

لفت أنتباهي البارحة وأثناء البحث في غوغل عدم وجود أي موضوع باللغة العربية تطرق إلى مقارنة الـ IPv4 مع الـ IPv6 لذا دعوني أكون أول واحد يقدم هذه الخدمة لأخواننا العرب كون الموضوع مهم ومعقد بعض الشيء للبعض. وقبل أن أبدا المقارنة أحب أن أقول أن هذا الموضوع ليس مقارنة بالمعني الحرفي لان أغلبنا يعلم جيدا الـ IPv4 ويعلم محتوياته ومميزاته وسوف يكون الموضوع بشكل عام هو توضيح لمميزات الـ IPv6 لكن على شكل مقارنة مع الـ IPv4

IPv6	IPv4
يستخدم الأيبي 128بت أي حوالي 16بايت	يستخدم الأيبي 32بت أي حوالي 4بايت
يوفر (شد حيلك قبل ماتقرأ الرقم) 340,282,366,920,938,463,463,374,607,431,768,211,456 وهذا يعني لكل شخص فيني سوف يحصل على 5×1028 أيبي فقط	يوفر 4,294,967,296أيبي وعدد كبير منها يستخدم لأهداف معينة مثل Privet IP و Multicast الخ.
لايوجد شيء أسمه Broadcast على الأطلاق وتم أستبداله بي IP Multicast لعمل Flood على كل الأجهزة الموجودة على الشبكةوهو FF02::1	يستخدم Broadcast لعمل Flood على كل الأجهزة الموجودة على الشبكة.
تم أزالة قسم الـChecksum من الـHeader وسوف يتم الأعتماد على الـChecksum الموجود على الـLink Layer او الموجودة في الطبقات الأعلى أي على TCP, UDP الخ.	يحوي الـHeader على قسم خاص بي الـChecksum
لايتطلب لأعداده كتابة أي شيء فهو يستطيع أن يولد لنفسه أيبي بشكل أوتماتيكي ويمكنه العمل مع وبدون DHCP سيرفر	أعداده يتم بشكل يدوي أو من خلال DHCP سيرفر
يوفر تقنية نقل جديدة تعرف بي Anycast والتى توفر سرعة أكبر في النقل وتوفير في الباندويدث	غير مدعومة بمثل هذه التقنية
تم أزالة قسم الـ Option من الـ Header مع توفير extension headers يوفر لك حيز في حال وجود بعض الخيارات التى يجب أضافتها	يحوي الـ Header قسم خاص بي الـ Option
تم توقيف Arp Protocol عن العمل وحل محله Multicast Neighbor Solicitation	يستخدم Arp Protocol للحصول على ماك أدريس معين لأيبي أو العكس
خاصية الـ IPsec مبينة ضمن الـHeader	خاصية الـ IPsec موجودة ضمن الـ Option الموجودة على الـ Header ويتطلب أن يكون الطرفين معدان للعمل من خلالها
تم أزالة قسم الـ Fragmentation من الـHeader وتم ضمه إلى extension headers وهو يدار من خلال المرسل فقط	يحوي الـ Header على قسم خاص بي الـ Fragmen-tation وهي تتم أما من خلال المرسل أو من خلال الروتر
تم أضافة قسم جديد إلى الـHeader تدعى Flow Label وهي خاصة بي الـ QoS	لايوجد قسم لي Flow Label وتتم عملية QoS من خلال الروتر



وهذه صورة توضح Header كل بروتوكول على حدى وماهي التعديلات التى تم القيام بها

قسم أمن وحماية الشبكات

هذا القسم سوف يتم عرض فيه كل الأمور الواجب عملها في الشبكة بهدف التخفيف من نسبة القرصنة التى تحدث على الشبكة وأرجو منك أن تدقق على كلمة تخفيف لان النظرية العامة تقول لايوجد جهاز أمني خالي من الثغرات مهم كانت قوته!

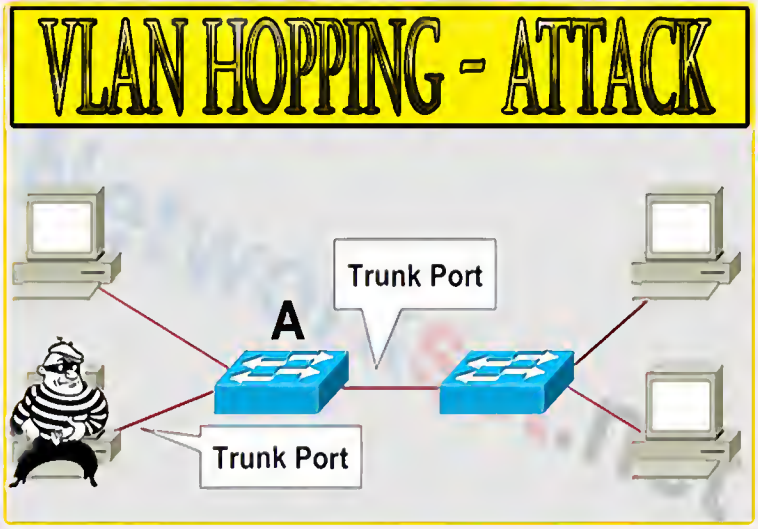
هجوم الـ Vlan Hopping وطريقة التصدي له

ماهو هجوم الـVlan Hopping ؟

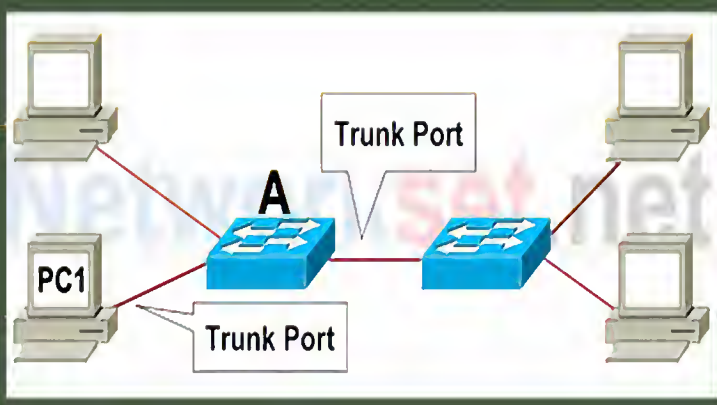
الهجوم الثاني الذي أريد أن أتحدث عنه ايضا يستهدف الـLayer 2 Devices ويدعى بي Vlan Hopping وتقوم فكرة هذا الهجوم باختراق قواعد الـ Vlan على الشبكة وذلك بالسماح لشخص معين موجود على Vlan2 مثلا بالدخولعلى Vlan 3 والاتصال بكل الاجهزة الموجودة هناك لاننا كما نعلم أن أحد مميزات الـ Vlan هي عزل الاجهزة عن بعضها البعض وينقسم هذا النوع من الهجمات إلى نوعين

Switch Spoofing
Double Tagging

نتعرف على كل واحد منهم



الطريقة الأولى : Switch Spoofing



كما نعلم جميعا أن وظيفة الـ Trunk Port هي السماح بالأتصال بين جميع الـ Vlans الموجودة في السويتش مع نفس الـ Vlans الموجودة على سويتش آخر وذلك بوسم كل Traffic ذاهب الى السويتش الآخر برقم الـ Vlan التى أرسلت منه وهذا بدوره يعطي الـ Trunk Port القدرة على الأتصال بكل الـ Vlans الموجودة على الشبكة لنتخيل أول

حالات هذه الهجوم

يقوم العابث الموجود على PC1 بعمل سويتش وهمي أو يقوم بوصل سويتش حقيقي على الجهاز مخبر السويتش Aبأنه Trunk Port وهذا بدوره يعطي العابث الصلاحيات في الوصول إلى كل الأجهزة الموجودة على الشبكة بالأضافة إلى أمكانية التنصت على كل الباكيت المرسلة بين الـVlans والسبب طبعا لان البورتات الموجودة في السويتش A تكون في حالة auto مع الطرف الآخر فهو يستجيب لك أذا أخبرته أنك سويتش وأنك Trunk Portوللتصدي لهذا النوع تقوم بكتابة أمر واحد على كل Interface موصول مع Host

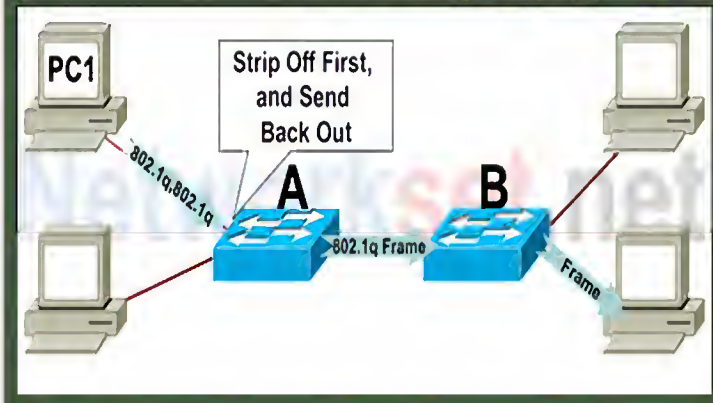
```
SwitchA#conf t
SwitchA(config)#interface fastethernet 0/1
SwitchA(config-if)#switchport mode access
```

بهذا الأمر نكون قد أوقفنا نصف الهجوم لان السويتش يحوي ثغرة أخرى تتم عن طريق بروتوكول الـ DTP أو Dynamic Trunk Protocol وظيفة هذا البروتوكول بأختصار هي تحديد نوع الـ Trunk Protocol الذي يجب أستخدامه بشكل أوتماتيكي أي تحديد هل يجب أستخدام 802.1Q أو ISL وهو يعمل Be default على كل البورتات الموجودة على السويتش وهذا مايستغله العابث بشكل جيد فهو يقوم بأرسال DTP Packet إلى السويتش مخبرا اياه بأنه يستخدم بروتوكول 802.1Q مثلا ليتحول الـ Port إلى Trunk Port بشكل أوتماتيكي حتى لو كنا قد طبقنا الأمر السابق ولأيقاف هذه البروتوكول عن العمل نقوم بتنفيذ الأمر التالي

```
SwitchA(config)# interface fastethernet 0/1
SwitchA(config-if)# switchport mode trunk
SwitchA(config-if)# switchport nonegotiate
```

وفيه أخبر البورت بأن لايقوم بالتفاوض مع الطرف الآخر حول نوع البروتوكول الذي يجب أستخدامه وبالتالي قمت بتوقيف عمل البروتوكول المسؤول عن عملية التفاوض مع الطرف الآخر وهو طبعا DTP Protocol ن خلال كتابتي للأمر الثالث switch port nonegotiate

الطريقة الثانية : Double Tagging



فكرة الطريقة الثانية أجمل من الأولى لانها تسمح للعابث للوصول إلى Vlan آخرى حتى لو قمنا بعمل كل الخطوات السابقة وهي ببساطة تقوم على مبدأ أرسال باكيت تم وسمها مرتان بي 802.1Q tags وعندما تصل الباكيت الى السويتش A يقوم السويتش بأزالة الـ Tag الخارجي فقط ويقوم بأرسالها الى السويتش B كا untagged packet وعندما تصل إلى السويتش B تصل وهي تحمل الـ Tag الداخلي الذي تم أعداده من قبل وليقوم السويتش بعدها بأيصال الباكيت إلى المكان المطلوب يمكن التصدي لهذا النوع من الهجوم بأرسال كل باكيت Untagged إلى Vlan تم أعداده مسبقا وغير مستخدمه لأي شيء ويتم ذلك من خلال الأمر التالي:

أولا يجب أن أقوم بأضافة Vlan وأخترت الرقم 210-بشكل عشوائي

```
SwitchA(config)#vlan 210
SwitchA(config)# interface fastethernet 0/1
SwitchA(config-if)# switchport trunk native vlan 210
```

في الأمر الثالث أخبر البورت بأن يرسل أي باكيت تعد Untagged إلى الـ Vlan 210

كلمة آخيرة أحب أن أضيفها وهي أن جميع هذه الأوامر مترابطة مع بعضها البعض ويجب تنفيذها جميعا حتى نستطيع أن نوقف هذا النوع من الهجوم الخبيث .

مقارنة بين سيرفرا التصاريح RADIUS & TACACS+

بقلم: أيمن النعيمي

تعتبر هذه السيرفرات من الأشياء المهمة في الشبكة والتى توفر لك حيز جيد من الأمان والحماية لشبكتك وللمستخدمين الموجودين عليها وهي تعتمد على خاصية تعرف بي AAA وتعني authentication, authorization, and accountability وهي خاصية موجودة في جميع أنواع الروترات وبعض الأنواع من السويتشات ووظيفتها الرئيسية أعطاء التصاريح للدخول إلى الشبكة بالأضافة إلى تحديد الصلاحيات لكل شخص يدخل على الروتر.

لنتعرف الآن على أهم الفروقات بين السيرفران

RADIUS server	TACACS+ server
سيرفر مفتوح المصدر ويمكن أستخدامه مع كل الأجهزة ومن بينها أجهزة سيسكو	سيرفر خاص بأجهزة سيسكو فقط
يستخدم بروتوكول الـ UDP والذي بدوره يجعل توصيل التصاريح بشكل أسرع من الـ TCP بالأضافة إلى وجود برمجة خاصة على السيرفر تتيح إعادة أرسال التصاريح في حال أنقضاء الوقت المسموح به	يستخدم بروتوكول الـ TCP المعروف بخاصية connection-oriented transport الذي تضمن وصول التصاريح بشكل جيد
يقوم بتشفير كلمة السر فقط	يقوم بتشفير عملية الأرسال بشكل كامل وهذا يشمل كل المعلومات المرسل من وإلى السيرفر ومن بينها أسم الدخول وكلمة السر والتصاريح المرسلة
لا يستهلك كثيرا من حجم الذاكرة الموجودة على الروتر ولا من قوة الروتر	أستهلاك أكبر للذاكرة وللمعالج الموجود على الروتر
يقوم بدمج الـ authentication, authorization بخطوة واحدة	يتعامل مع كل خاصية بشكل مستقل وهذا يشمل الخواص الثلاث
التصاريح فيه محدودة وتتمثل بتصريح واحد وهو privilege mode والسبب طبيعا هو دمج الـ authentication, authorization مع بعضهم البعض	يدعم كل التصاريح الموجودة على الروتر أي انه يتيح 15تصريح مختلف
لايدعم البروتوكولات التالية Apple-Talk,Novel,NetBios,X.25	يدعم كل انواع البروتوكولات

وطبعا بعد قراءتك لكل هذا الفروقات سوف تستنتج أن سيرفر TACACS+ هو الأفضل بلا منازع إلا انا الواقع العملي يقول ان أستخدام الـ RADIUS أكثر من أستخدام الـ TACACS+ والسبب على ما أعتقد هو أن الأول هو مفتوح المصدر والذي يتيح للمستخدمين خيارات أكثر عند الأستخدام.

متى أختار RADIUS ؟

نختار RADIUS أذا كنا من مناهضي البرامج المفتوحة المصدر والذي تعطي أيضا سبب كبير لأستخدام هذا النوع من السيرفرات والسبب أمكانية التعديل على الكود المصدري

نختار RADIUS في حال كنا نتعامل مع أجهزة مختلفة المنشأ وهذا يشمل كل الأنواع ومن بينها سيسكو وجونيبر

نختار RADIUS في حال كان يهمنا الأداء أو الـ Performance الخاص بالروترات لان الـ RADIUS يعمل بشكل أخف من TACACS+.

متى أختار TACACS+ ؟

نختار TACACS+ عندما يكون موضوع الأمن مهم عندنا على الشبكة لان الـ T+ ACACS يقوم بتشفير عملية التبادل بشكل كامل بالاضافة إلى أمكانية التحكم بمستوى التصاريح المعطاة للمستخدمين

نختار TACACS+ عندما تكون الشبكة عندنا تعمل مع بروتوكولات مختلفة مثل AppleTalk,Novel,NetBios,X.25

نختار ACACST+ عندما تكون المرونة شيء مطلوب على الشبكة والسبب طبعا هو استخدامنا لي الـ TCP والذي يعطي مرونة اكبر للشبكة من خلال استخدامه خاصية three-way handshake

Cisco Systems

RAM	256 MB (installed) / 1 GB (max)
Flash memory	64 MB (installed) / 256 MB (max)
Type	Router
Connection Type	Ethernet, Fast Ethernet, Gigabit Ethernet
Encryption Algorithm	DES, Triple DES, AES
Supplied OS	Cisco IOS SP services
Voice Codecs	G.711, G.723.1, G.728, G.729, G.729a, G.729ab, G.726
IP Telephony Features	Echo cancellation (G.168)
Protocol Remot	SNMP 3
Interfaces	2 x network - Ethernet 10Base-T/100Base-TX/1000Base-T - RJ-45 ¦ 2 x USB ¦ 1 x management - console ¦ 1 x network - auxiliary
Firewall protection, 128-bit encryption, hardware encryption, VPN support, MPLS support, URL filtering, 256-bit encryption	

Cisco 2800 Series Voice Bundles (CISCO2851-CCME/K9)

RAM	128 MB
Flash memory	16 MB Flash
Type	stackable -Switch
Mac-Address Table	12000 Entries
Interfaces	48 x Ethernet 10Base-T, Ethernet 100Base-TX
Connection Type	Ethernet, Fast Ethernet
Data Rate	100 Mbps
Authentication method	Kerberos, Secure Shell (SSH), RADIUS, TACACS+
Protocol Remote	SNMP 1, RMON 1, RMON 2, SNMP, Telnet, SNMP 3, SNMP 2c
Routing Protocol	OSPF, IGRP, BGP-4, RIP-1, RIP-2, EIGRP, HSRP, IGMP, DVMRP, PIM-SM, static IP
Flow control routing, auto-sensing per device DHCP support, auto-negotiation, ARP support, trunking, load balancing, VLAN support, auto-uplink (auto MDI/MDI-X), IGMP snooping, manageable , IPv6 support	

Catalyst 3750 Series 10/100 Workgroup Switches WS-C3750-48TS-E

RAM	512 MB
Flash memory	64 MB Flash
Type	Security appliance
Connection Type	Ethernet, Fast Ethernet, Gigabit Ethernet
Interfaces	1 x network - Ethernet 10Base-T/100Base-TX - RJ-45 ¦ 1 x management - console - RJ-45 ¦ 2 x Hi-Speed USB - 4 PIN USB Type A ¦ 1 x serial - auxiliary - RJ-45 ¦ 4 x network - Ethernet 10Base-T/100Base-TX/1000Base-T - RJ-45
Encryption	DES, Triple DES, AES
Performance	Firewall throughput : 450 Mbps ¦ VPN throughput : 225 Mbps ¦ Connection rate : 12000 connections per second
Features	Firewall protection, VPN support, load balancing, VLAN support, High Availability
Concurrent sessions : 280000 ¦ IPSec VPN peers : 750 ¦ SSL VPN peers : 2 ¦ Virtual interfaces (VLANs) : 100	

Cisco ASA 5520 Firewall Edition ASA5520-BUN-K9 security appliance

Juniper NETWORKS

Aggregate Half-Duplex Throughput
* 10 Gbps

FPC Slots and Full Duplex Throughput **per Slot**
* 1 built-in, 4 Gbps additional 1 Gbps for FIC

PICs per Chassis
* 4, plus 2 additional fixed FE, or 1 fixed GE ports

Chassis per Rack
* 24

Redundancy
* No

Dimensions
* 3.5 x 17.5 x 18 in
* 8.9 x 44.5 x 45.7 cm

Mounting
* Front or center

Maximum Weight
* 38.2 lbs / 17.3 Kg

Power Options
* DC Input Power (Fully Loaded): 10 A at -48 VDC; 378 watts
* No. of power supplies required (non-redundant/redundant): 1/2
* AC System Input Power (Fully Loaded): 4 to 2 A; 100 to 240 VAC; 47 to 63 Hz; 400 watts

Router M7i

Number of Interfaces*
8 mini-GBIC (SX, LX or TX), or 2 XFP 10 Gig (SR or LR)

Maximum Number of IP Addresses in Trusted Interfaces
Unrestricted

Maximum Throughput
* 10 Gbps FW
* 5 Gbps 3DES VPN

Maximum Number of Sessions
1,000,000

Maximum Number of VPN Tunnels
25,000

Maximum Number of Policies
40,000

Maximum Number of Virtual Systems
0 default, upgradeable to 500

Maximum Number of Virtual LANs
4094

Maximum Number of Security Zones
16 default, upgradeable to 1,016

Maximum Number of Virtual Routers
3 default, upgradeable to 503

Routing Protocols Supported
OSPF, BGP, RIPv1/v2

High-Availability Modes Supported
* Active/Passive
* Active/Active
* Active/Active Full Mesh

IPS (Deep Inspection FW)
Yes

Integrated / Redirect Web Filtering
Yes

NetScreen-5200

Maximum Performance and Capacity	Network Connectivity	Routing, Virtualization, Encapsulations
* **Junos Software Version Support: Junos Software 9.1**	* Fixed I/O: 4 x 10/100/1000	* BGP, OSPF, RIP, Static, ECMP: Yes
* **Firewall Performance (Large Packets): 600 Mbps**	* Maximum PIM Slots: 3	* Multicast, PIM SM, SSM,IGMP: Yes
* **Firewall Performance (IMIX): 400M**	* Maximum EPIM Slots: 0	* Maximum Number of Security Zones: 40
* **Firewall and Routing PPS (64 Byte): 175, 000 pps**		* Maximum Number of Virtual Routers: Yes
* **3DES and SHA-1 VPN Performance: 140 Mbps**		* Maximum Number of VLANs: 256
* **Concurrent VPN Tunnels: 512 MB / 1 GB DRAM 256 / 512**		* PPP, FR, MLPP, MLFR, HDLC: Yes
* **Maximum Concurrent Sessions: 512 MB / 1 GB DRAM 64 K / 128 K**		
* **New Sessions/Second: 5,000**		

Router J2320

Data Rate
* 480 Gbps

Throughput
* 357 Mpps (wire speed)

10/100/1000BASE-T Port Densities
24 (dual-mode 1/10GbE network ports)

10GBASE-X Port Densities
24

100BASE-FX / 1000BASE-X (SFP) Port Densities
N/A

Resiliency
Dual load-sharing internal autosensing AC power supplies

Power Options
Autosensing; 110/220 VAC; 60/50 Hz

Operating System
JUNOS

QoS Queues / Port
8

Traffic Monitoring
N/A

MAC Addresses
16,000

Jumbo Frames
9216 Bytes

IPv4 Unicast / Multicast Routes
N/A

Number of VLANs
1,024

Switch EX2500

مصلحات تقنية

TCP : وتعني Transmission Transfer Protocol وهو أحد البروتوكولات التى تنتمي إلى الطبقة الرابعة Transport Layerويستخدم مع بروتوكول الـIP ووظيفته الرئيسية هي نقل البيانات في الشبكة العنكبوتية وأكثر مايميزه هو مراقبة نقل البيانات بين المستقبل والمرسل والتأكد من وصول جميع البيانات بشكل صحيح من خلال القيام بعملية الـThree-Way Handshake

UDP : وتعني User Dtatgram Protocol وهو البروتوكول الثاني الذي أيضا يستخدم في نقل البيانات وطبعا ينتمي إلى الطبقة الرابعة ويميزه سرعة النقل بين الأجهزة ويعيبه أنه لايقوم بالتأكد من وصول البيانات بشكل صحيح لذا نجد أستخدامه ينحصر في نقل الصوت والفيديو

DNS : وتعني Domain Name System وهي خدمة تقوم بترجمة أرقام أسماء المواقع إلى أيبيات تستطيع من خلالها أجهزة الكمبيوتر التواصل مع السيرفرات التى تحوي هذه المواقع والسبب لان الأنترنت بشكل عام يتعامل مع الأرقام أي صفر وواحد كما أنها أيضا تتيح التعرف على الأسم من خلال رقم الأيبي ويمكن أختصارها إلى أنها مركز الأستعلام الذي يوفر لك معلومات عن كل أسم أو أيبي

DHCP : وتعني Dynamic Host Configuration Protocol وهو بروتوكول يعمل في الشبكة ويقوم بتزويد الأجهزة بكل المعلومات اللازمة للأتصال مع الشبكة وهذا يشمل ايبي وماسك وجيت واي بالأضافة إلى DNS ويشترط على الأجهزة وجود DHCP Client يقوم بالأتصال مع السيرفر ويحصل على كل المعلومات اللأزمة

FTP : وتعني File Transfer Protocol ويمكن ترجمتها إلى العربية إلى بروتوكول نقل الملفات وهو بروتوكول يسهل عملية نقل الملفات بين الأجهزة من خلال سيرفر خاص فيه ويستخدم البورت 21-للنقل كما يتطلب من الأجهزة التى تريد أن تقوم بنقل الملفات من السيرفر إلى أجهزتها وجود FTP Client

Telnet : وتعني Terminal Network وهو أحد بروتوكولات الشبكة المعروفة ويستخدم للأتصال والتحكم بأجهزة السيرفر والكمبيوتر على الشبكة العنكبوتية ويعمل من خلال بروتوكول الـTCP ويستخدم البورت 21-ويعيبه أنه يقوم بأرسال الأوامر من دون أي نوع من التشفير إلى الجهاز المستقبل

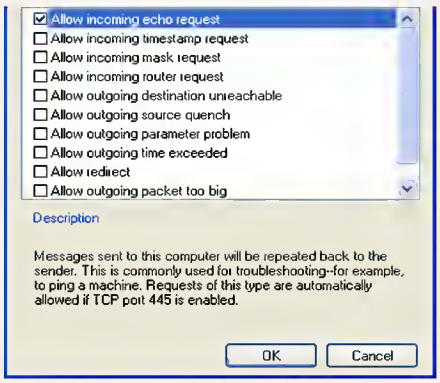
ARP : وتعني Address Resolution Protocol وهو يعد Computer Networking Protocol ويعمل في الطبقة الثانية Link Layer ووظيفته الرئيسية الحصول على عنوان الماك أدريس لأيبي معروف وذلك لأتمام عملية الأتصال معه أو القيام بعكس العملية أي الحصول على ايبي لماك أدريس معلوم من خلال بروتوكول رديف له يدعى Inverce ARP

HTTP : وتعني Hyper Text Transfer Protocol وهو احد البروتوكولات التى تعمل في الطبقة الأولى Application Layer ويستخدم لنقل البيانات في الشبكة العنكبوتية WWW ويتطلب وجود برنامج وسيط يقوم بهذه العملية ومثال عليه برامج التصفح مثل فايرفوكس وأنترنت أكسبلورير ويعيبه أن يقوم بأرسال البيانان من دون أي تشفير بعكس بروتوكول HTTPS الذي يقوم بتشفير جميع البيانات بين المرسل والمستقبل

مشاكل وحلول

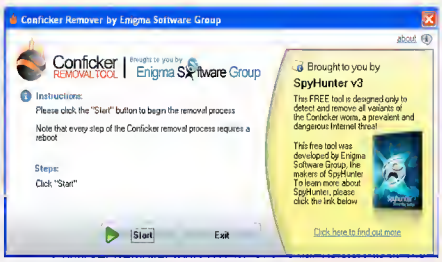
سوف يتم تخصيص هذا القسم لعرض المشاكل التى قد تواجهك في الشبكة بالأضافة إلى طريقة حل المشكلة كما أرحب أيضا بأرسال مشاكلكم على بريد المجلة magazine@networkset.net للنظر فيها وتقديم أفضل الحلول لها .

مشكلة : لماذا الـPING لايعمل في شبكة مؤلفة من جهازين كمبيوتر وقد تم التاكد من طريقة التوصيل وأرقام الأيبي؟



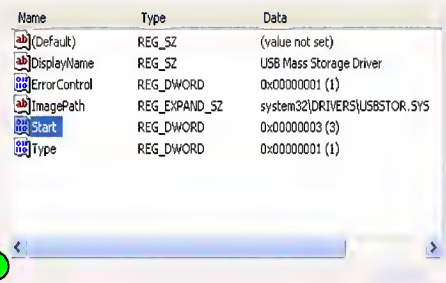
الحل : هذا النوع من المشاكل يحدث غالبا بسبب وجود الجدار الناري الموجود مع ويندوز والذي يقوم بشكل أوتماتيكي بمنع كل رسائل الـICMP من الدخول إلى الجهاز ولحل هذه المشكلة لدينا طريقتان الأولى وهي أيقاف عمل الجدار الناري بشكل كامل ويتم ذلك من خلال الدخول إلى لوحة التحكم وبعدها إلى إعدادت الجدار الناري ووضع المؤشر على خيار إيقاف أو OFF الطريقة الثانية تتم بأضافة Exceptions أو أستثناء للجدار الناري لكي يسمح بعبور رسائل الـICMP ويتم الأمر من خلال التوجه أيضا إلى لوحة التحكم وبعدها إعدادت الجدار الناري وبعدها نضغط على خيارات متقدمة أو Advanced وبعدها نختار ICMP ونضع المؤشر كما هو موضح بالصورة على خيار Allow incoming echo request على كلا الجهازين

مشكلة : السيرفر عندي لا يفتح أغلب مواقع الحماية ومضادات الفايروس مثل Kaspersky,Norton, ؟



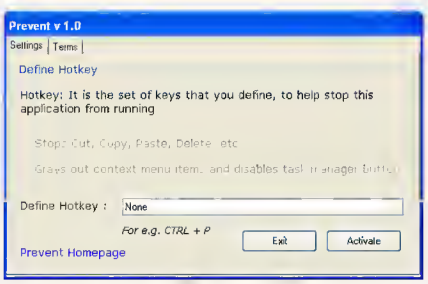
الحل : تحدث هذه المشكلة بفعل فايروس أوكراني الصنع ويدعى كونفكير أو Conficker يقوم هذا الفايروس بأغلاق أغلب مواقع الأنتي فايروس بالأضافة إلى موقع مايكروسوفت والكثير من المواقع الهامة أيضا للقضاء عليه يجب عليك أن تقوم بتحميل أداة خاصة تقوم بحذف الفايروس وتدعى Conficker Removal Tool1.0.0.16 وهي أداة مجانية تستطيع أن تجدها من خلال أستخدام البحث في غوغل

مشكلة : كيف أقوم بأغلاق كل فتحات الـ USB على جهاز الكمبيوتر ؟



الحل : قم بالتوجه إلى إبدا أو Start وبعدها قم بالضغط على تشغيل وقم بكتابة regedit للوصول إلى مسجلات الكمبيوتر وبعدها توجه إلى العنوان التالي HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR وإبحث عن هذا التسجيل Start وقم بتغيير قيمته من 3- إلى 4وهي تشير إلى تعطيل كل المخارج ولو في حال أردت أن تقوم بنفس الموضوع على مستوى الشبكة تستطيع أن تنفذ هذا الأمر من خلال عمل بوليسي على مستوى الشبكة

مشكلة : كيف أقوم بمنع النسخ واللصق على جهاز الكمبيوتر وعلى الشبكة أيضا ؟



الحل : لكي تقوم بأيقاف كل أشكال النسخ والصق على جهاز الكمبيوتر لدين طريقتان الأولى الدخول على الريجستري والقيام بالتعديل على بعض المسجلات الخاصة بكل أمر والطريقة الثانية وهي أيضا تعتمد على المسجلات لكن تتم من خلال برنامج صغير جدا يدعى Prevent 1.0 يقوم بأيقاف كل أشكال النسخ والصق بالأضافة إلى أختصارات لوحة المفاتيح تستطيع أن تجدها على محرك البحص غوغل .

بالنسبة لمنع النسخ على الشبكة فهي تتم من خلال سيرفر مخصص يثبت على ويندوز سيرفر و يدعى Rights Management Services وهو يقوم بأضافة صلاحيات لكل ملف من بينها صلاحيات النسخ واللصق والطباعة ويعيبها أنه لايدعم كل أنواع الملفات الموجودة فهو يدعم ملفات الأوفيس والأدوب أكروبات وسوف يكون له موضوع كامل في المستقبل